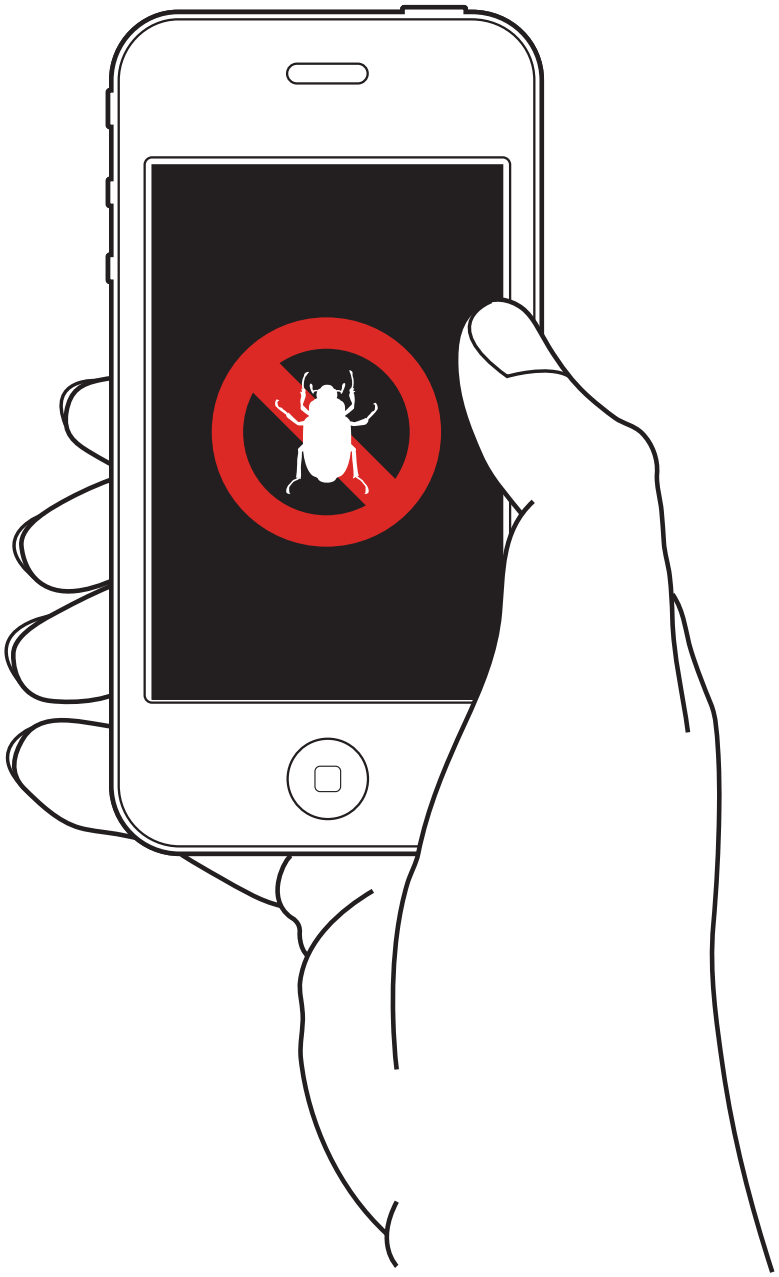
FORTINET®

2014 Threat Landscape Report

2014 Threat Landscape Report

FORTINET®

Contents



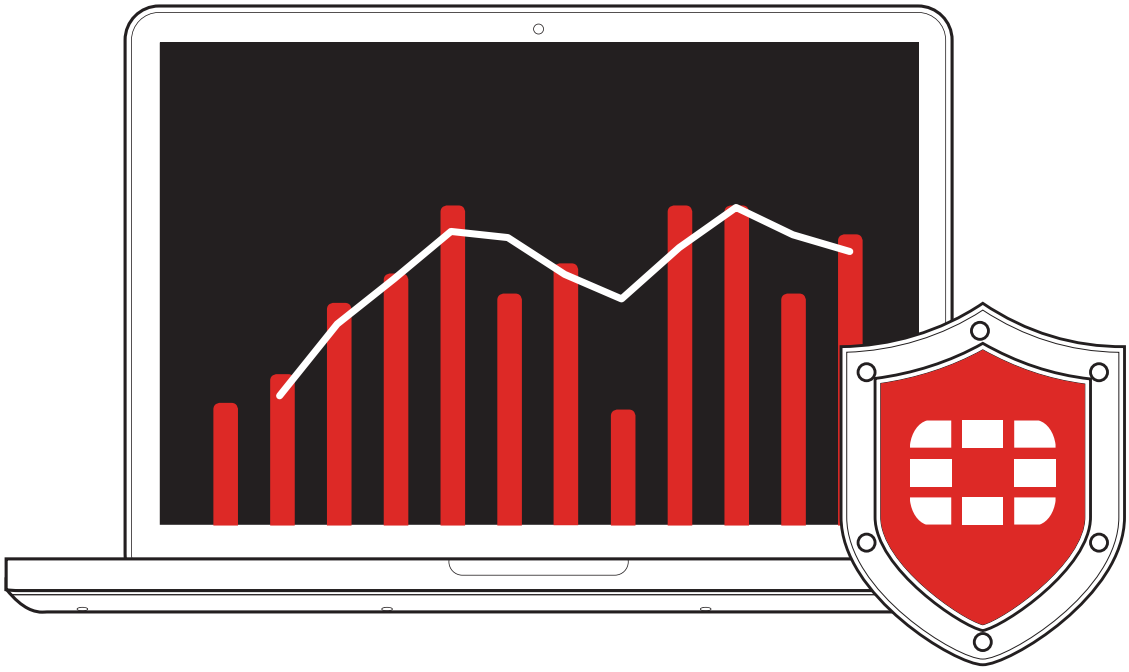
4 Foreword

5 Executive Summary

6 Malware

12 Mobile Malware

20 Botnets



26 Web

30 Spam

34 FortiGuard Labs

38 About Fortinet

39 References

At Fortinet, our goal is to help our customers build the most secure environment they can in order to succeed.
As technologies advance, and more and more devices connect to the Internet, the opportunities for those that may wish to inflict harm have increased exponentially.
Only a few years ago, devices like smartphones were the exclusive domain of the very technologically advanced and business people wanting around the clock access to their email. Fast forward to today, and the world is a new place: smartphones are no longer the exception but the norm, and portable computing driven by affordable tablet devices are rapidly entering new markets once untouched by personal computing.

Criminals have not let this new world pass them by.
New users to the Internet, especially in developing markets, haven't had the years of exposure to the Internet many of us take for granted. Phishing emails, spam links, pirated software are all terms unfamiliar to many people in the world eagerly unwrapping their new devices and joining us online. Malware authors have noticed, and 2013 saw unprecedented growth in the amount of mobile malware Fortinet collected. We expect this trend to continue in 2014, with new and novel ways of infecting mobile devices to continue unchallenged - except in cases where companies and users have taken the proactive steps to implement a robust BYOD strategy as well as educate themselves on the threats online in the mobile world.

The Advanced Persistent Threat continues to target businesses and governments.
Often designed and executed by the best of the best, these well-funded advanced attackers will stop at nothing to penetrate a target and execute their goals: state secrets, corporate espionage and theft of sensitive data are all goals of APT actors. Only companies with a layered defence strategy can hope to detect these attacks in time to staunch the flow of data from their networks.

The scale of information theft continues to exceed all predictions.
Years ago, Information Technology was seen as a cost center for businesses, and not a cost saver. Through the years that attitude has changed, and allowed companies to move parts of their operations online, build new marketplaces and grow their businesses to new levels. Information Security has trailed behind IT - often seen as an afterthought. Recent breaches of tens of millions of customer's sensitive financial information has shed a new spotlight on security and the need for companies to build a comprehensive security posture to defend against the inevitable attacks on their systems.

At Fortinet, we are proud to offer you a hand in building systems that can help defend your networks from attack, and I am excited to present to you a small piece of the efforts our FortiGuard Labs team has accomplished in 2013.

Regards,

Chief Technology Officer,
Fortinet

Executive Summary

Malware

Malware continues to menace computer networks around the world - from the home user to the enterprise, malware leaves no stone unturned in its goal to enrich its masters. 2013 saw both good news and bad: some key figures in the malware world were apprehended, while new threats such as Cryptolocker taught many - the hard way - to maintain better backups of their data.

Mobile Malware

The past year saw an explosion of growth in mobile malware, and almost all of it was focused on breaching the ubiquitous Android platform. More and more people around the world have embraced new devices - many have never been online before. Malware authors have used this growth in new devices to expand their wares into a enw world, and the rampant growth shown proves it.

Botnets

ZeroAccess ruled the botnet roost in 2013, but ended the year with a white flag and a whimper as a coordinated effort to finally take down one of the largest botnets ever built seems to have been successful. But botnet owners are a wily bunch: old botnets and bot malware once thought dead or dormant have shown signs of resurrection.

Web

FortiGuard Labs maintains a database of over a quarter of a billion website and URLs, covering almost 80 unique categories. This allows customers to easily build customized access profiles for their users to ensure they only visit the resources online they should.

Spam

Spam continues to be a huge percentage of all traffic traveling the Internet today. Spammers send literally billions of messages in the hopes that a pittance will make it past antispam technologies and a user will click on a link. In 2013, spammers used resources all over the globe to launch their campaigns.

FortiGuard Labs

Since it began actively researching zero-day exploits in software in order to better protect customer networks, FortiGuard Labs has responsibly disclosed 142 vulnerabilities to vendors, of which 18 were discovered in 2013. Our highly-skilled and adept antivirus analysts contributed 19 papers in 2013 to the publication *Virus Bulletin*, the industry standard in antivirus research.

Malware:

Better, Smarter, Faster, Stronger

Malware has long been seen as a menace to computer users around the globe, and **2013 was no exception to that rule:** malware authors continue to embrace practices that mirror the practices of legitimate businesses. The affiliate model of spreading infections has made both cybercriminals and their middlemen very wealthy[1].

Malware that was once the exclusive domain of a select few – those that were willing to pay malware authors for exclusive use of specialized tools and customized exploits – has become **commoditized** and available for the use of cybercriminals of all stripes.

Mobile malware has seen a dramatic rise in infections and development. While aging mobile phone operating systems like Symbian continue to be targeted, Android received the most attention by attackers.We'll take an in-depth look at the rise in mobile malware in **Section 4**.

2013 saw a year of cyclical change in the number of attempted attacks; as new exploits and tools were made available to the cyber underground, FortiGuard Labs saw a spike of incidents. Once these spikes were abated, we saw a brief lull in new infections, only to have another round of fresh attacks **leveraging recently patched exploits and vulnerabilities**.

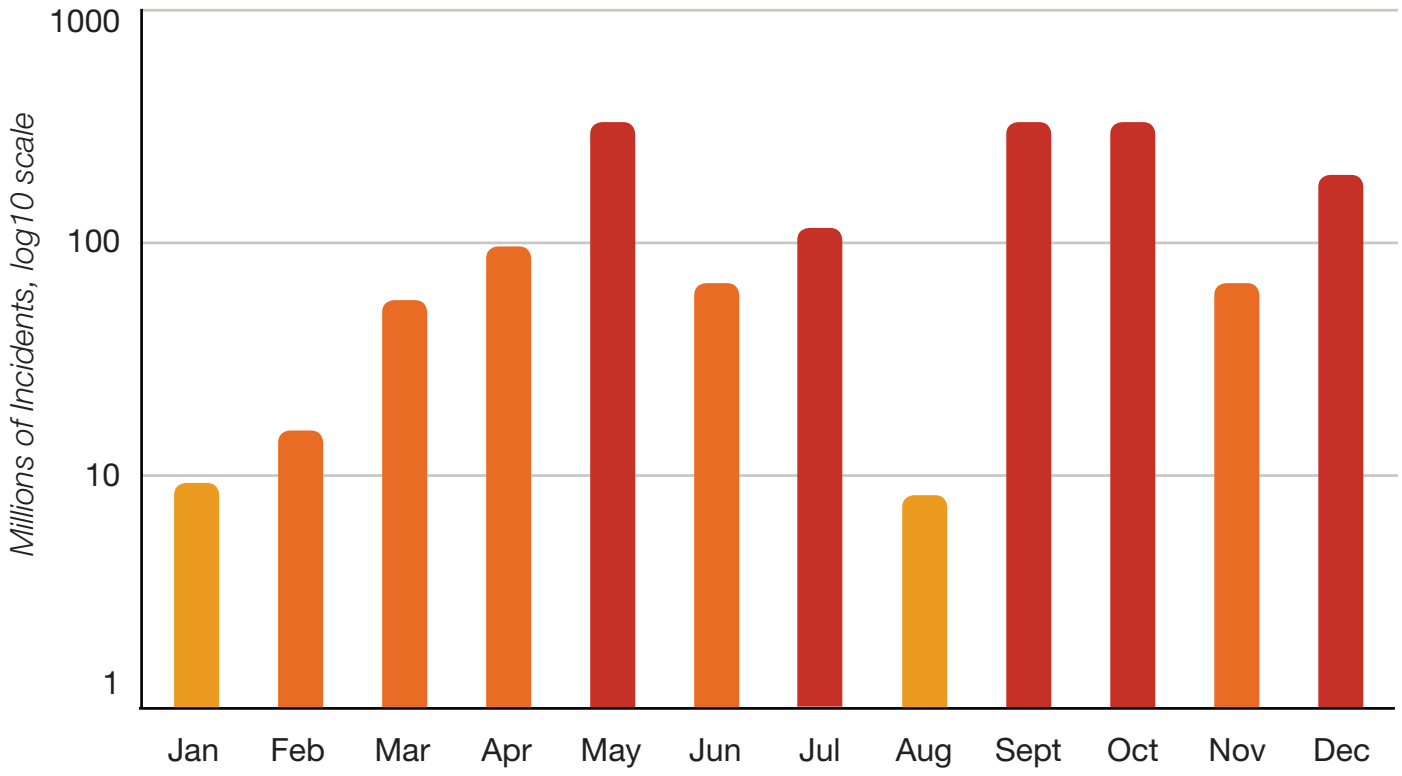
Of particular note, in mid-2013 the world was introduced to the newest version of ransomware – **Cryptolocker.** While ransomware in general isn't new, Cryptolocker's author took heed to where previous versions of ransomware failed and developed a new version that was incredibly successful[2].

There were some silver linings to the abundance of storm clouds raining down on the Internet last year, though: a programmer who goes by the handle of **Paunch** – in apparent self-deprecating reference to his ample waistline – was apprehended by Russian authorities in October[3]. Paunch is the purported creator of the **Blackhole Exploit Kit** – perhaps the most successful malware delivery software ever created. Paunch also authored the **Cool Exploit Kit**, a very expensive kit that was rented to a very select group of customers at great expense. For the most part, both Blackhole and Cool have gone silent in the aftermath of his arrest.

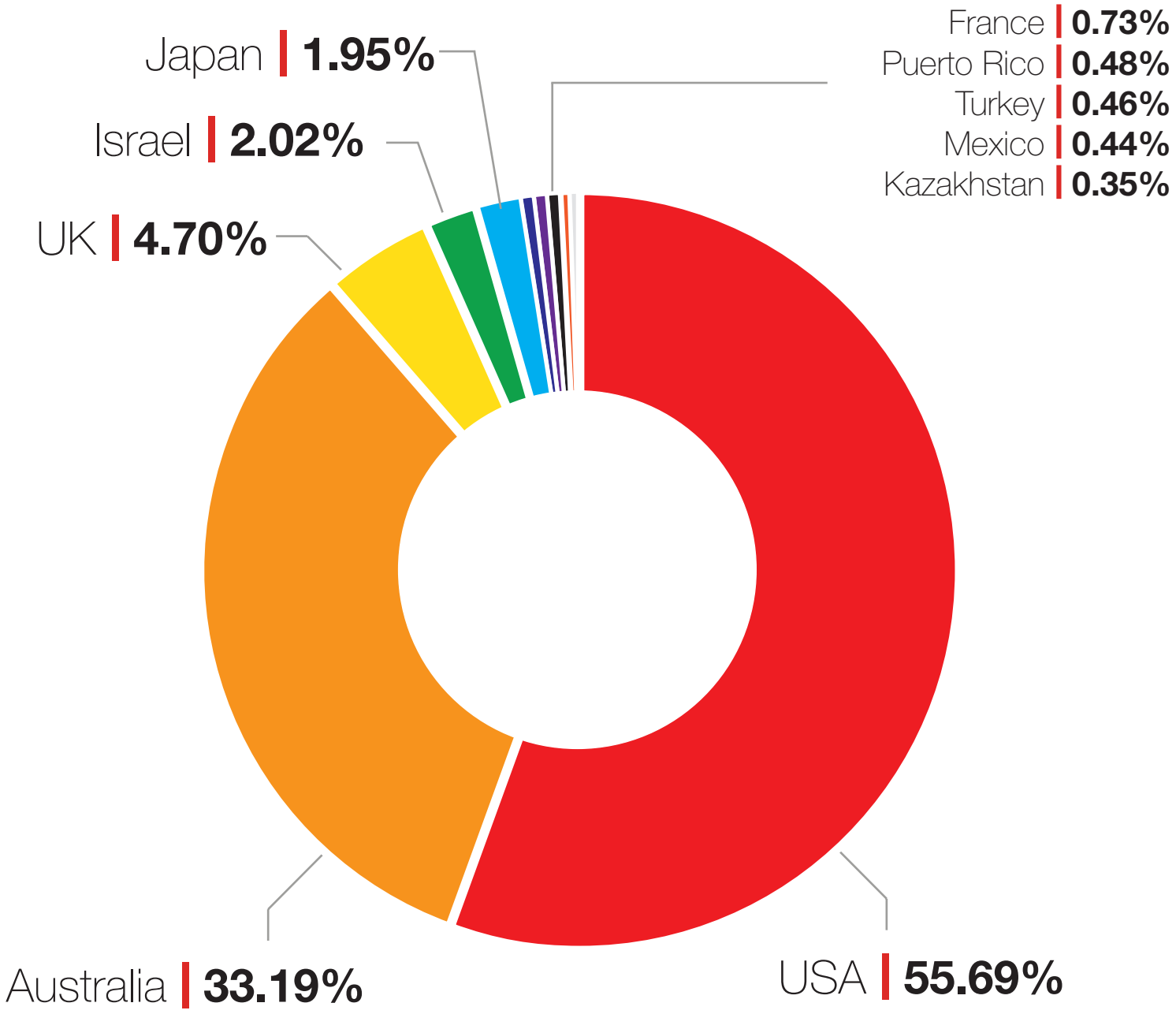
In January of last year, 24 year old Algerian hacker Bx1 was apprehended in Thailand on behalf of US authorities for being the mastermind behind an alleged 5 year attack spree on hundreds of banks and other financial institutions using the popular ZeuS and SpyEye trojans. **Authorities claim that he was able to abscond with over $100 million over the 5 years**[4].

Finally, in April, authorities in Ukraine arrested a massive 21-person strong group of cybercriminals responsible for the highly successful Carberp banking trojan. **Carberp was marketed as a DIY financial trojan for aspiring criminals**, and was sold for as much as $40,000. It was estimated that up to $250 million was taken from victims during Carberp's reign[5]. One interesting turn of events after the arrests were made came to light in June: **the source code to the trojan was leaked**[6] and available for anyone to review. While this was beneficial to researchers and malware analysts, it also meant that anyone with the desire to roll their own malware based on Carberp could do so.

Malware incidents reported to FortiGuard Labs

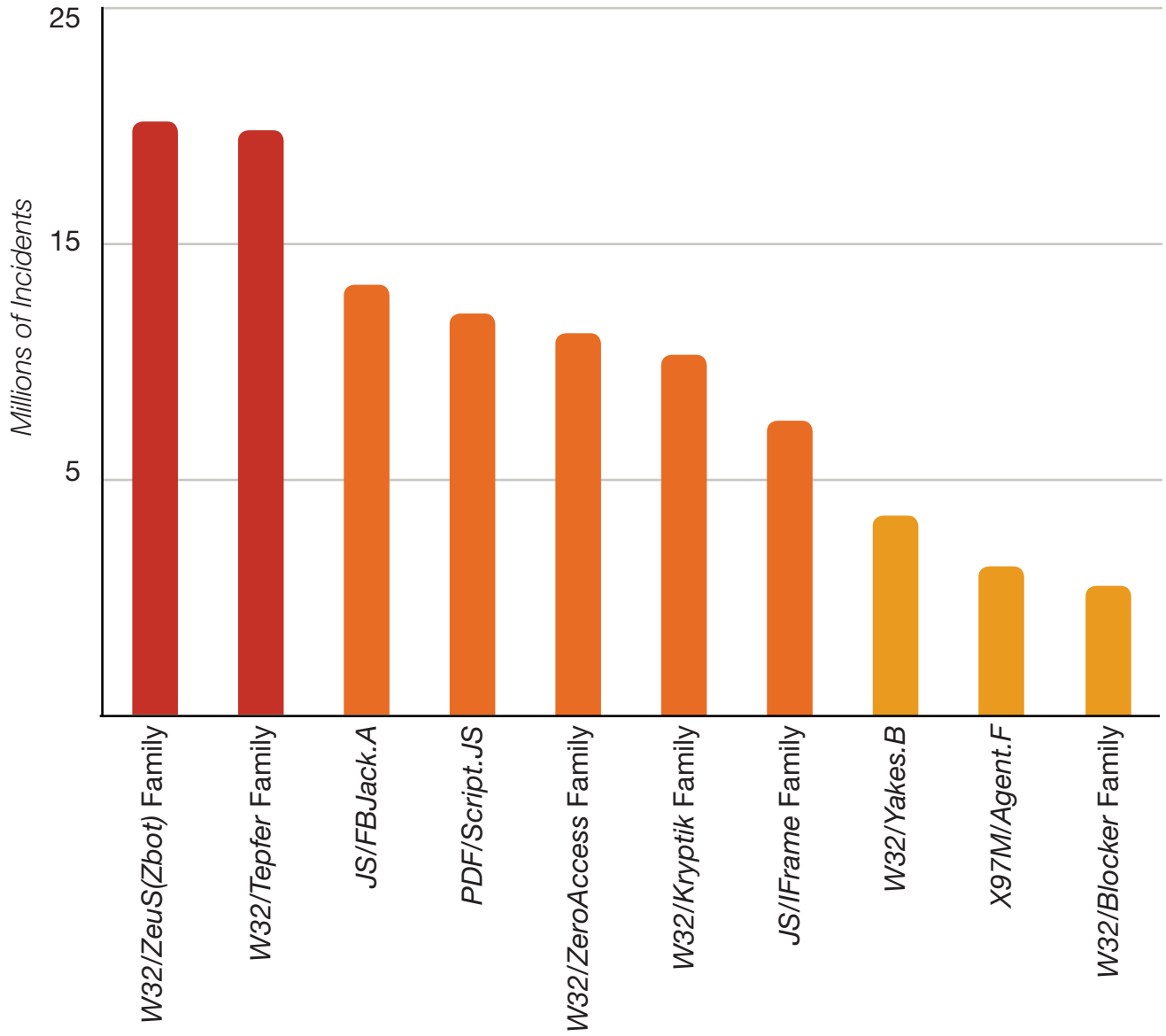


Over the year, malware incidents showed a cyclical trend of new infections over the year: January and August showed lower incidents of events as people turned off their PCs for extended vacations, only to fall prey to massive spikes in malware in the months after. The month of May saw a thirty times increase in incidents over January, which we attribute to the success of ZeroAccess and Blackhole, as well as the worldwide success of Darkleech compromising Linux servers to deliver malware to unsuspecting website visitors[7]. On both the desktop and server front, many of these successful infections are due to the lack of urgency shown to patch software and operating systems: Exploit Kit authors were seen in 2013 to roll out new versions of their wares sometimes within a day of a vulnerability being patched and details made public. The final months of 2013 also saw a massive spike in incidents recorded: the success of new versions of ZeroAccess, despite the best efforts of Symantec in July to throw a wrench in the works[8], led to millions of new attempts to infect computers.



Total incidents, top 10 countries, 2013

Top 10 Malware Families Reported, 2013



Malware authors in 2013 created many different headaches for both computer users and network administrators. Multiple vectors were used by cybercriminals in the hopes of successfully delivering their malicious payloads: from exploit kits to macro viruses, attackers tried every door knob expecting to find one of them unlocked.

The stalwart ZeuS trojan took the top spot in 2013, with over 20 million attempts to infect FortiGate-protected networks. ZeuS first showed up on computers in 2007, and has been a thorn in the side of Internet users ever since. The 2011 leak of ZeuS's source code led to an explosion of copy cat variants by aspiring cybercriminals looking to make their fortunes on the backs of innocent victims[9].

The Tepfer family of ransomware closely trailed ZeuS in attempts to infect computers in 2013; thousands of variants were used to target users around the world with a fake alert screen from a local law enforcement organization demanding payment of a 'fine' in order to release control of the victim's computer. Tepfer was designed to prevent the victim from accessing their desktop or file system by intercepting key processes and terminating them.

An interesting and nefarious development late in 2013 saw ZeuS infections being used in a new way: while ZeuS was often used as a financial trojan, a significant number of ZeuS infections were used to deliver and execute the Cryptolocker ransomware. Cryptolocker put a new spin on ransomware: it used uniquely generated cryptographic key pairs to fully encrypt the contents of a victim's computer, **and any mapped drive the victim had the ability to write to**. Cryptolocker would then inform the victim they had a short period of time to pay a significant ransom - sometimes as much as a few hundred dollars, and typically only paid using the Bitcoin cryptocurrency - before the encryption key used to encrypt the victim's computer was deleted, **making the victim's files completely unrecoverable**. Victims ranged from home users losing thousands of personally significant files like photographs, to businesses of all sizes and public agencies. Cryptolocker was also seen to infect users via other methods: infected flash drives, often in combination with fake program activation tools commonly spread through file-sharing sites and through infected email attachments.

It appears that Cryptolocker may be the work of a single person or a very small group of criminals: a Ziff Davis investigation in December traced Bitcoin payments to a handful of addresses that accepted payment from victims. In the last 3 months of 2013 alone, a staggering number of Bitcoins were paid to the hostage takers, with a rough value of almost **30 million dollars**[10].

Recent high profile arrests of cybercriminals leads us to have hope for the same in 2014 - will law enforcement agencies be able to find the people behind these millions of attacks?

Mobile Malware:

More Phones, More Bots, More Profit

2013 provided a bumper crop for malware targeting mobile devices. The rapid growth of malware targeting Android continues to be of concern to system administrators who have implemented a BYOD strategy on their networks. FortiGuard Labs detected over **1,800 new distinct families of viruses** in the past year, and the majority of those are targeting Google's Android platform.

While attacks on platforms such as Symbian wane, **attackers have made Android OS the number one mobile target**. The NewyearL.B Android malware, which was bundled inside a seemingly harmless flashlight application, continued to target millions of devices. Unwitting or unaware users looking to try out the latest games or apps find themselves unknowingly sharing a wealth of personal information to an attacker, leading to obtrusive advertisements and other negative effects such as allowing NewyearL.B permission to add and remove system icons and modify and delete the contents of any external storage.

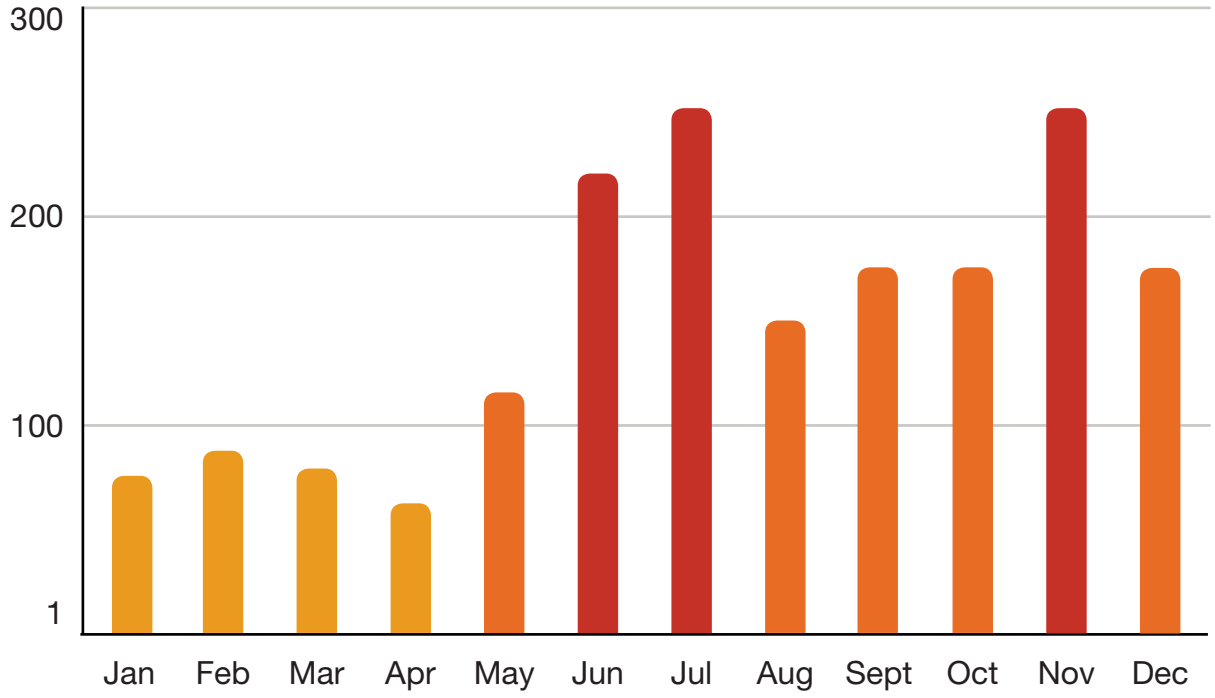
The distribution of Android malware continues to accelerate at a break neck pace: at the start of 2013 we collected just over 50,000 samples per day. We finished 2013 collecting around 450,000 on a daily basis. Clearly cybercriminals are putting a substantial amount of effort into churning out hundreds of thousands of new variants daily in the hopes that some of them will be successfully implanted on a target device.

Other malware targeting phones running iOS, BlackBerryOS, PalmOS and Windows were virtually non-existent. The number of incidents recorded by FortiGate devices in 2013 was infinitesimal in comparison to Android and Symbian.

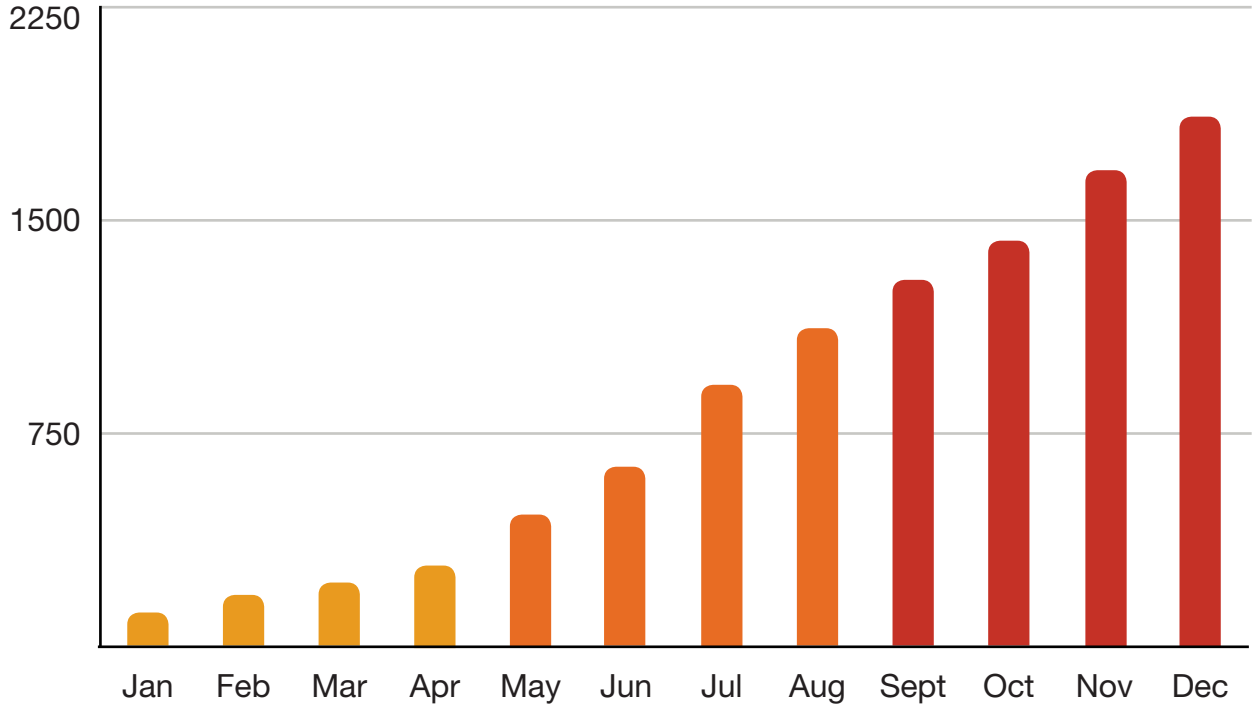
2013 also saw a new milestone in mobile malware: the first **ransomware** was found targeting Android. Ransomware, which has existed in various forms for well over two decades, typically holds your files on your computer 'hostage' and demands payment for their safe return. The Fake Defender malware (FortiGuard Labs detects this as Android/FakeDefend.A!tr[11]) uses some clever tricks in order to take control of its victim's phone and hold it hostage: first, it pays homage to the hugely successful Fake Antivirus malware on desktops by pretending to be an antivirus application called Android Defender. It then scares the victim into believing their phone is overrun with malware and then kills key processes and deletes a significant amount of files in the attempt to prevent the victim from restoring their phone from a backup file. Finally, after a short period of time the malware presents the victim with a special lock screen where the only option is to pay the attacker $99.99 via credit card for the "full" version of the antivirus software. In the case of Fake Defender, paying the ransom has no effect: nothing is downloaded and nothing is restored. The only option for the victim is to wipe the phone and start from scratch.

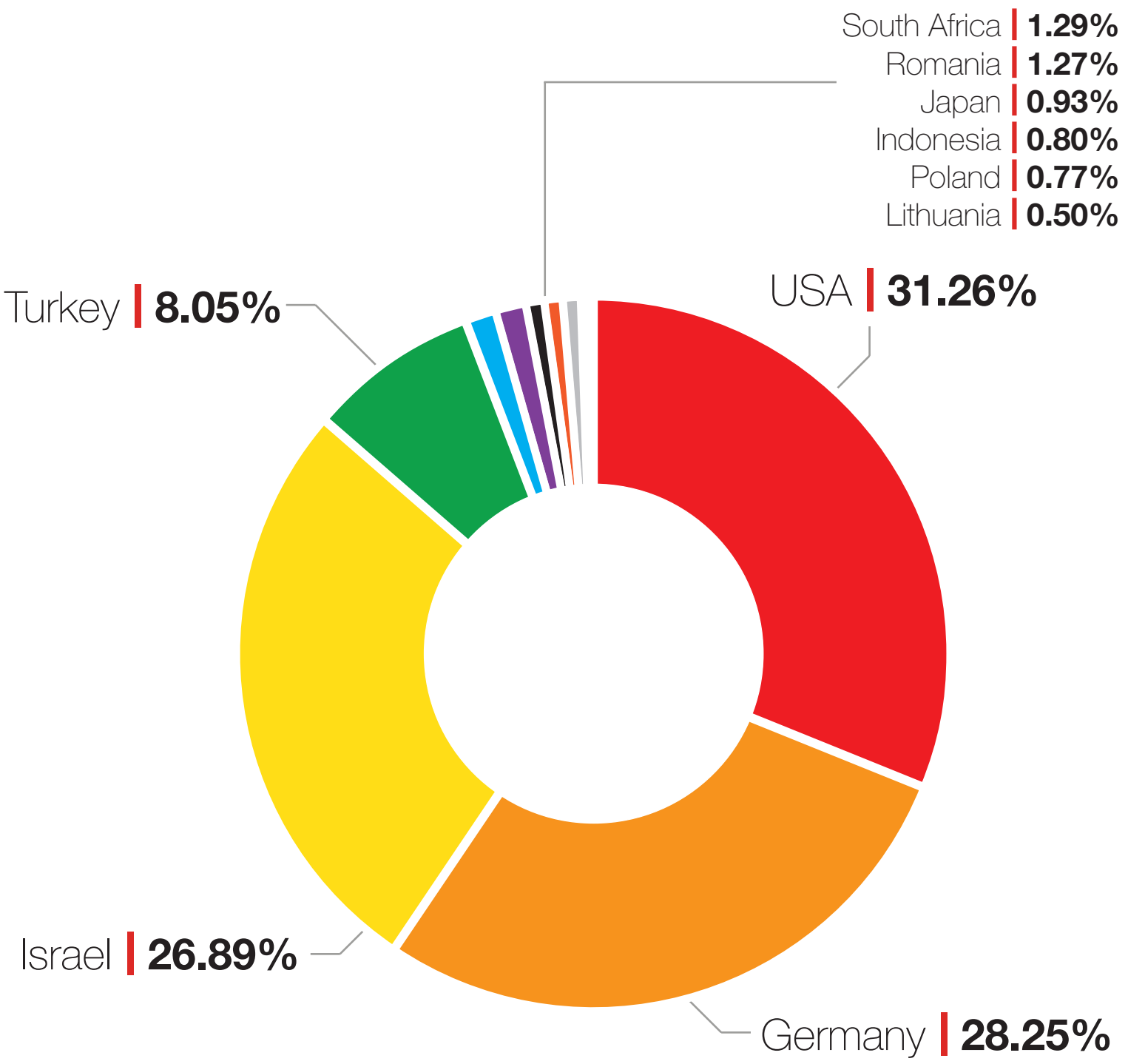
2013 also saw a new vector of infection for Windows: through Android. Android/Claco is disguised as a harmless 'cleaner' application, but when plugged into the victim's Windows PC, Claco attempts to autorun a malicious file it placed in the root of the phone's filesystem. The beginning of 2014 saw a new piece of Windows malware designed to infect Android devices. It's clear that malware authors are using every trick in the book in order to create new infections and spread their code, almost always for their personal gain.

Mobile Malware: New Distinct Virus Families Detected, 2013

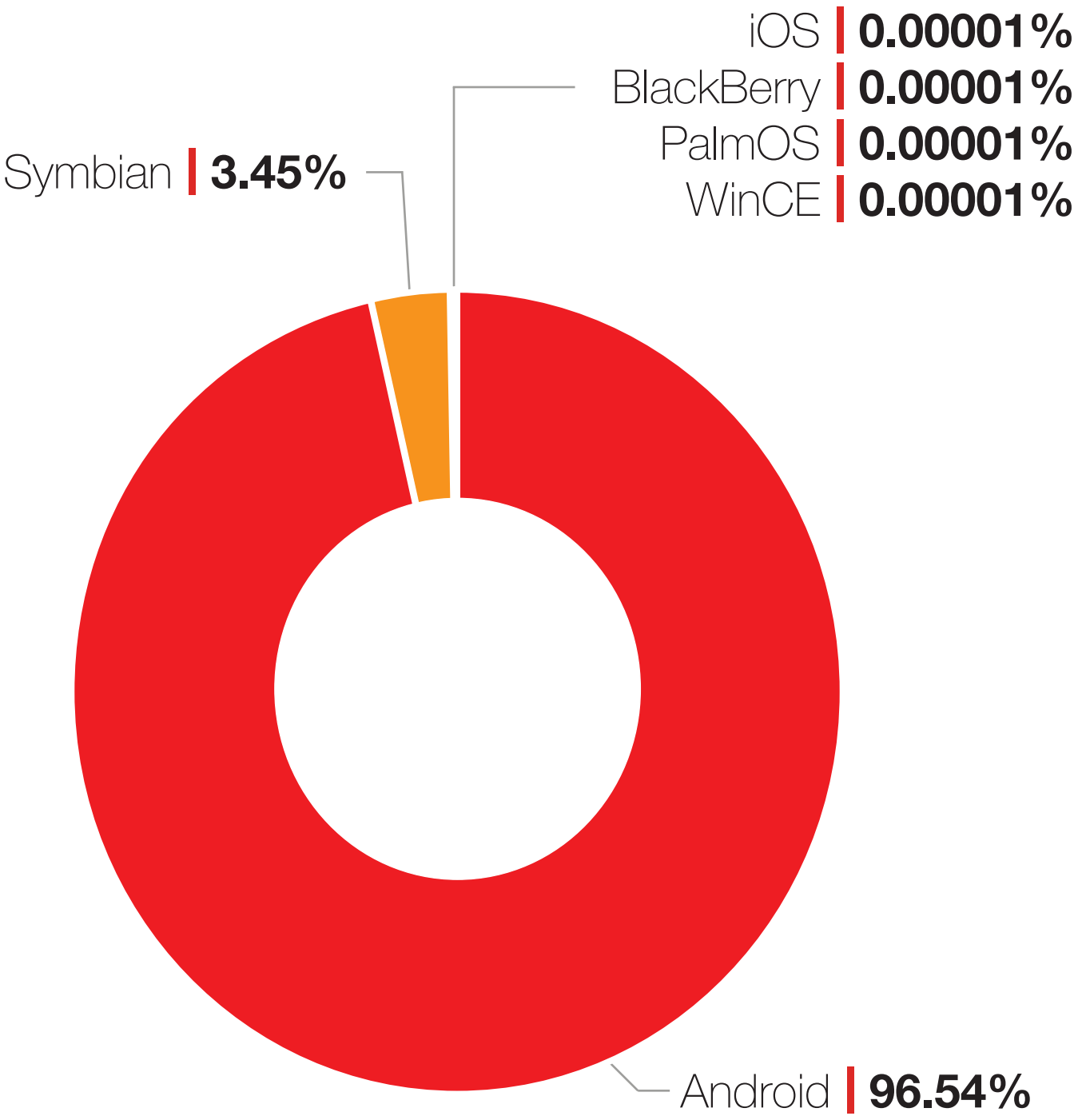


Cumulative Growth of New Mobile Malware Families, 2013



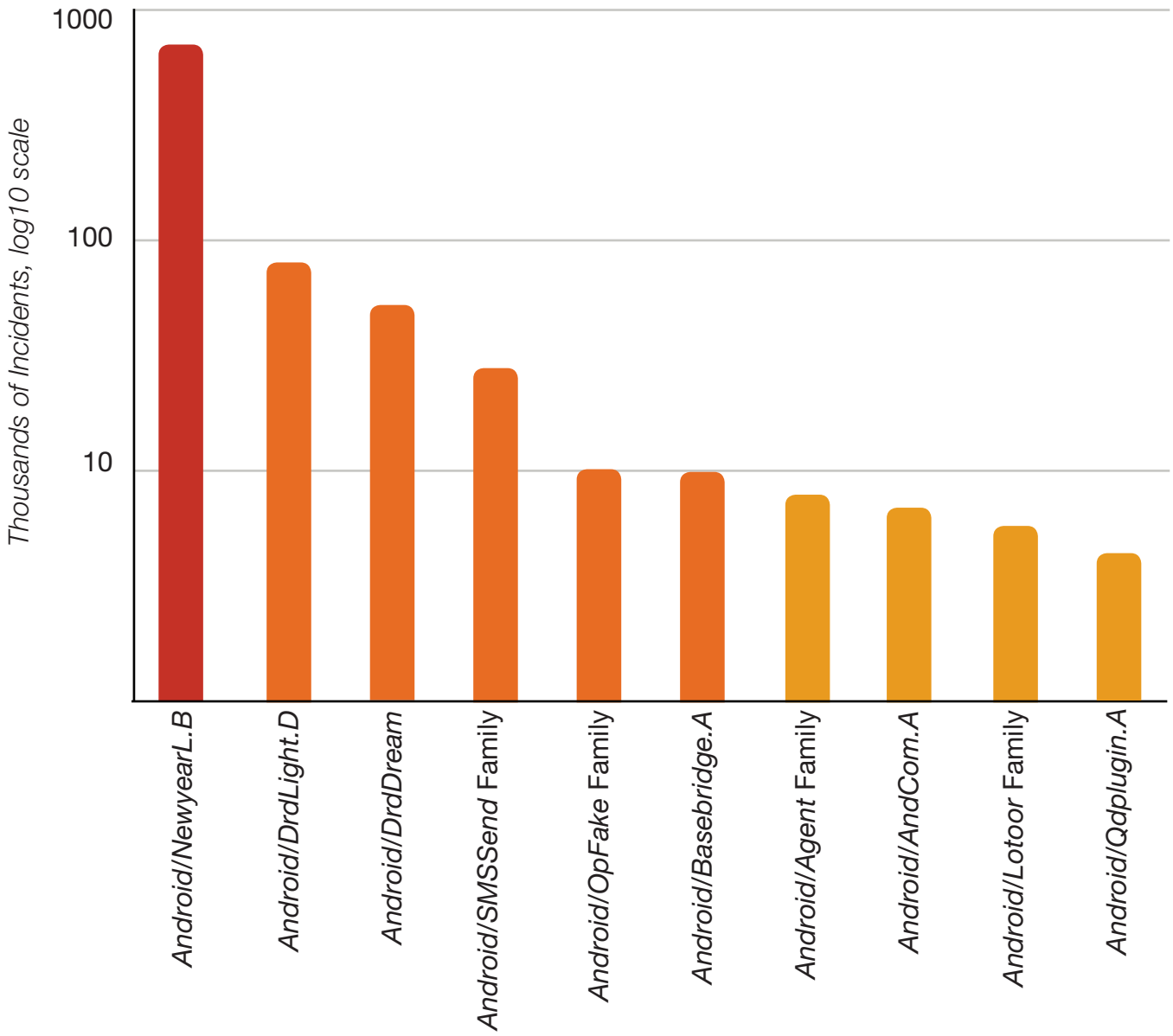


Total incidents, top 10 countries, 2013

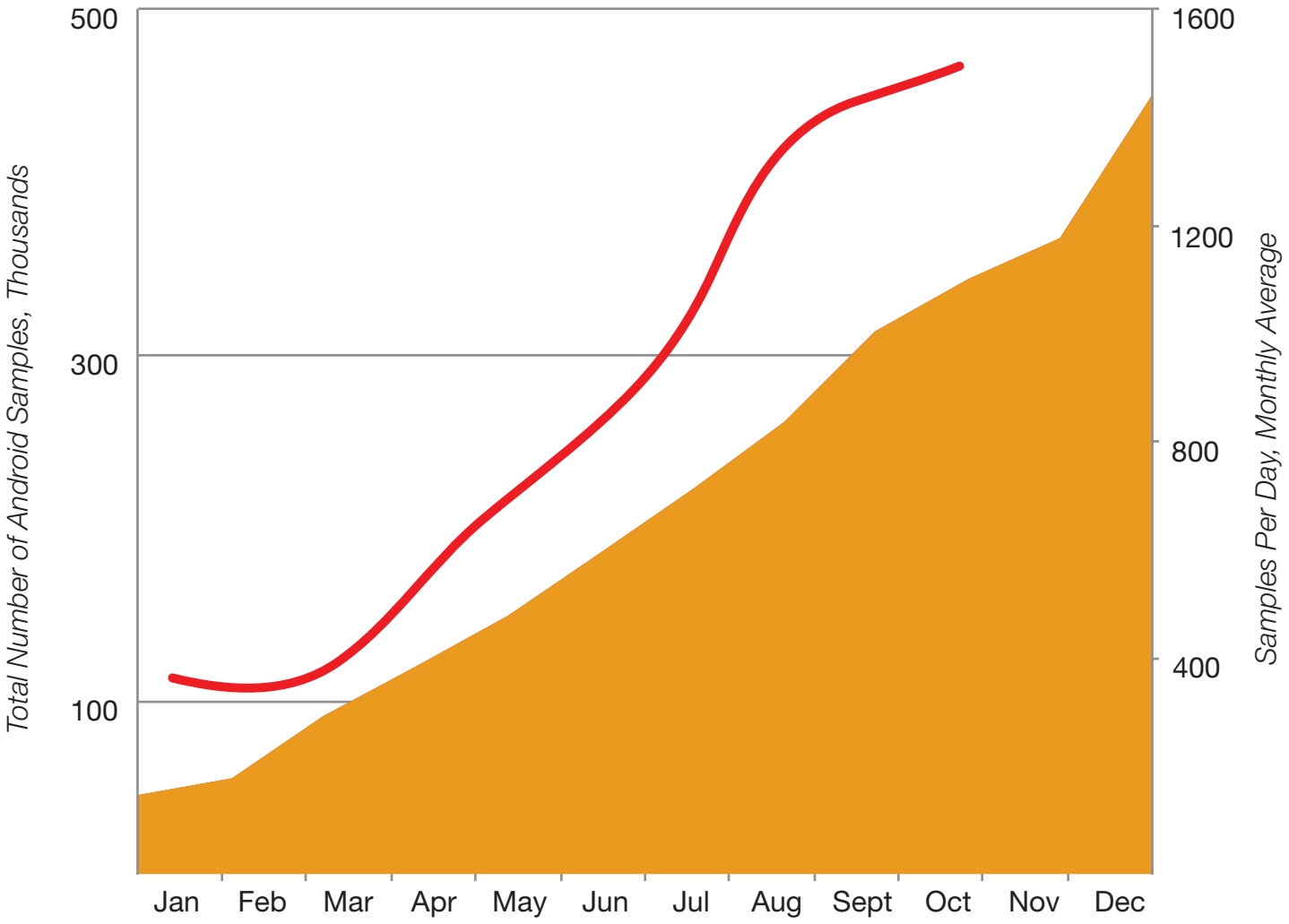


Prevalence of Mobile Malware Infections, 2013

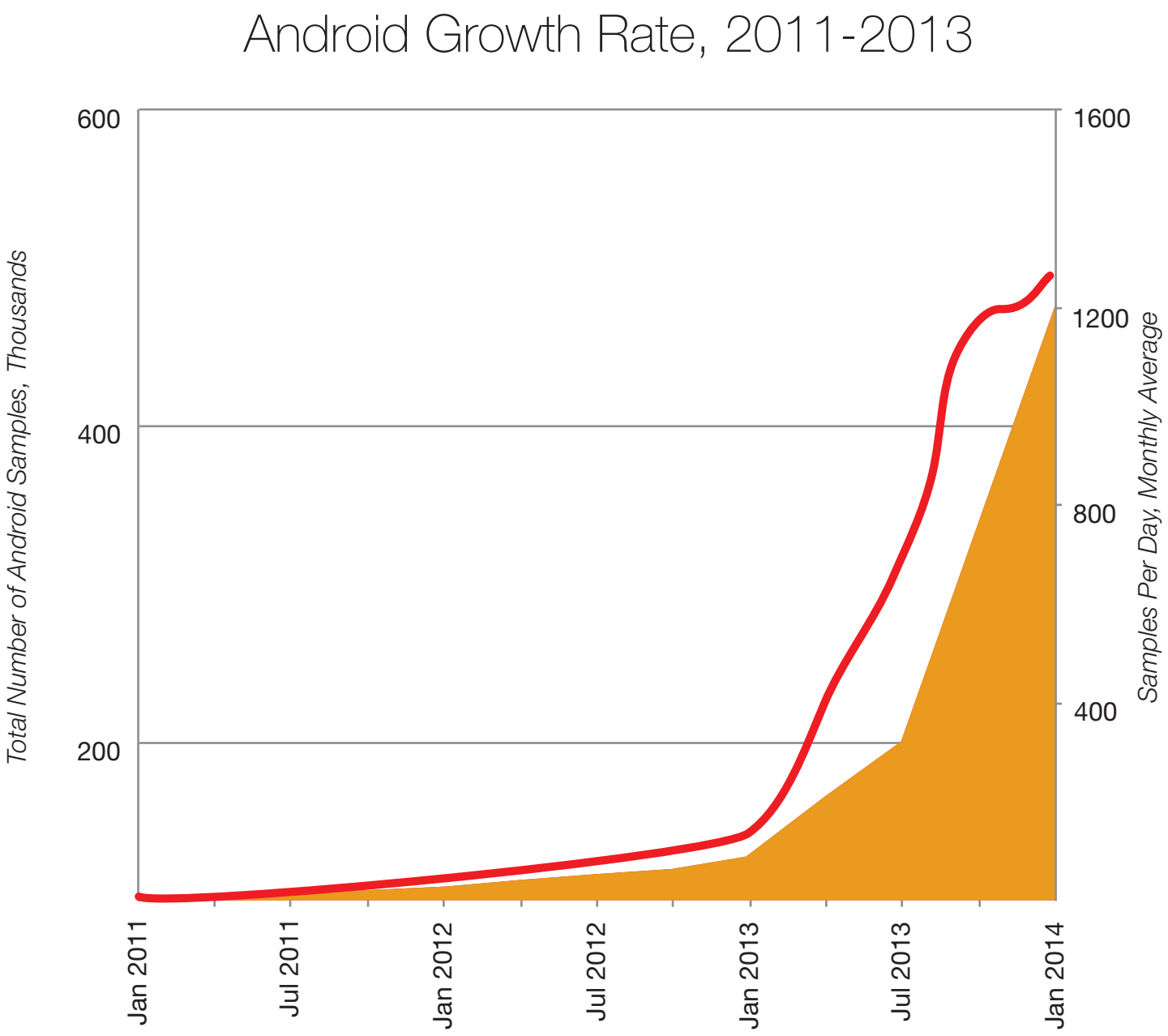
Top 10 Android Mobile Malware Families Reported, 2013



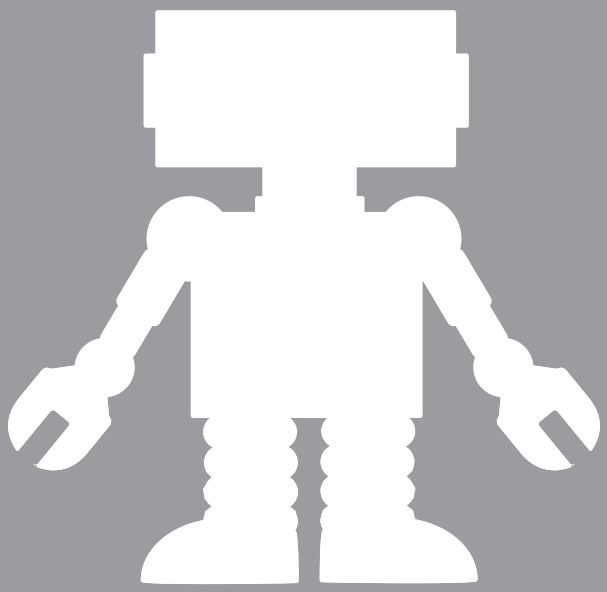
2013 Android Mobile Malware Samples



Looking at the growth of Android malware, we can see above that there is much to be concerned about going into 2014. The growth shows no signs of slowing; in fact, the growth seems to be accelerating. As more and more Android-based devices are purchased and taken online, the opportunities for attackers to infect increases as well. There are literally hundreds of low-cost Android devices available for purchase today - well within the reach of the developing world. Many of these new users are likely to have had very little, if any, exposure to the Internet. As these new users embrace their new phone or tablet, we expect a surge in new infections and incidents.



If we take a look back at the growth of Android malware over the past 3 years, we can see that 2013 became the year that mobile malware designed to target the Android platform flourished. Infections continue to accelerate, as do the number of samples FortiGuard Labs collects. As computer users continue to replace their desktops and laptops with smartphones and tablets, it's likely this upward trend will continue in 2014.



Botnets:

Everything Old is New Again

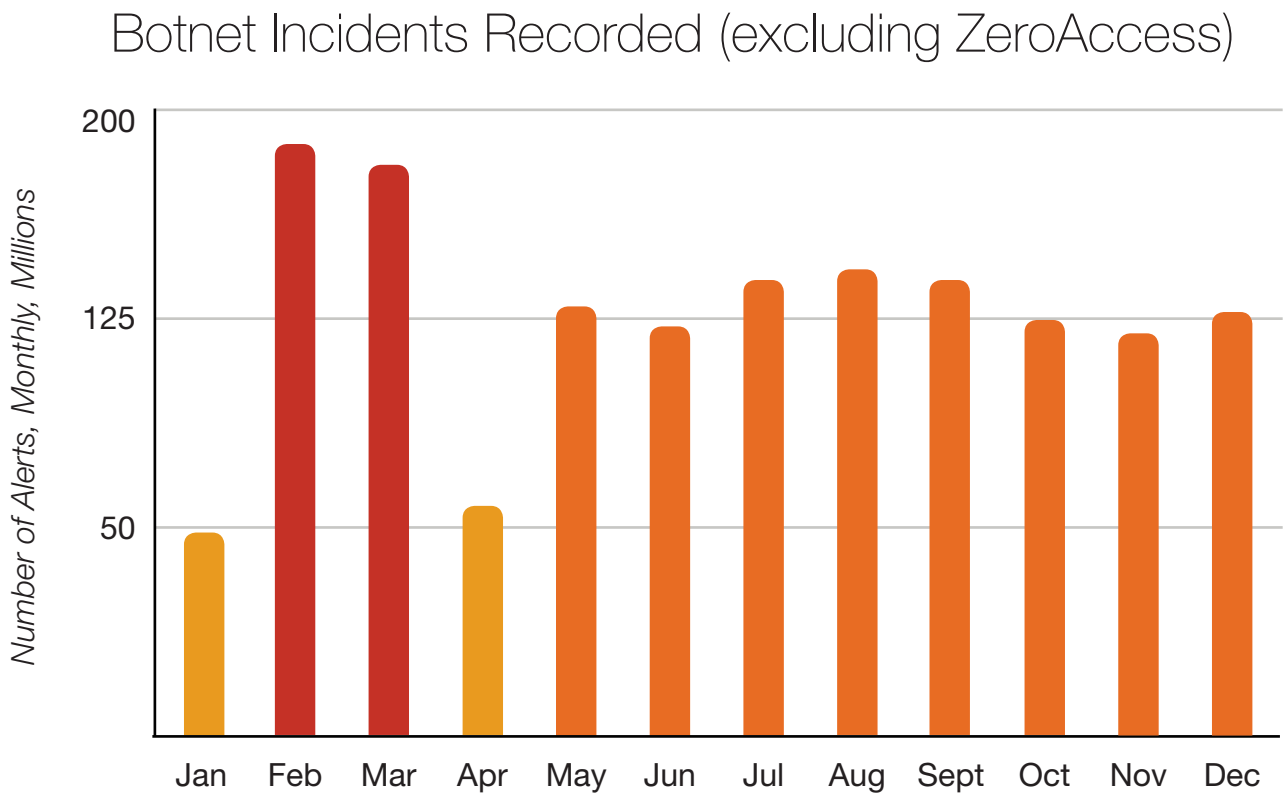
2013 saw some significant events in the world of botnets. Old botnets long dormant reappeared, and ZeroAccess - despite the best efforts of organizations to dismantle - showed an incredible amount of activity last year.

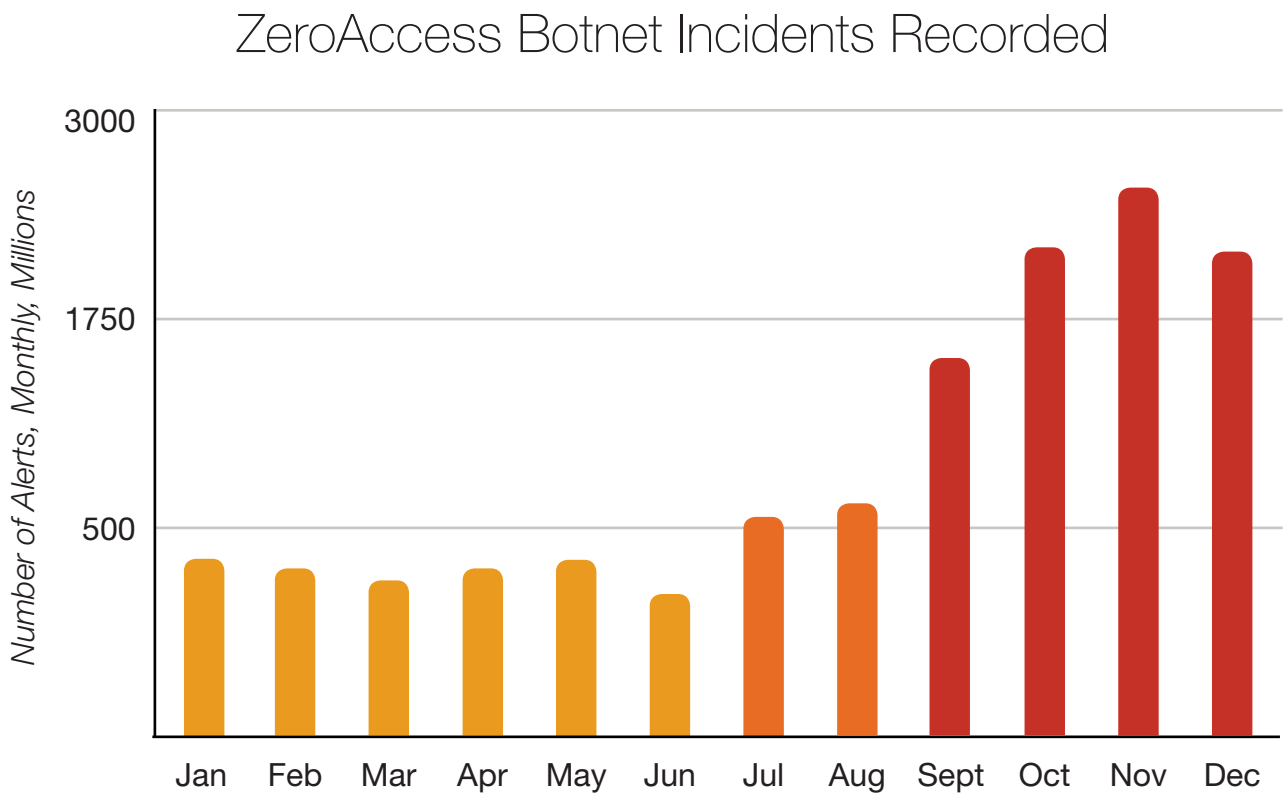
The Waledac botnet, infamous for its ability to send billions of spam emails daily, was taken down by Microsoft in 2010. Early in 2013, computers infected with Virut began downloading new copies of Waledac in order to **send thousands of spam emails** per day[12]. It's likely that malware middlemen were taking advantage of previously infected machines to 'double dip' their affiliate payouts. After all, if you can make a buck or two more by dropping a separate botnet onto a computer you've already infected, why think twice? We also saw a **resurgence of the famous DDoS Mariposa botnet**, although as a whole, its penetration was small. For a more in-depth look at how the malware affiliate model works, read our 2013 Cybercrime Report, located at www.fortinet.com/resource_center/whitepapers.

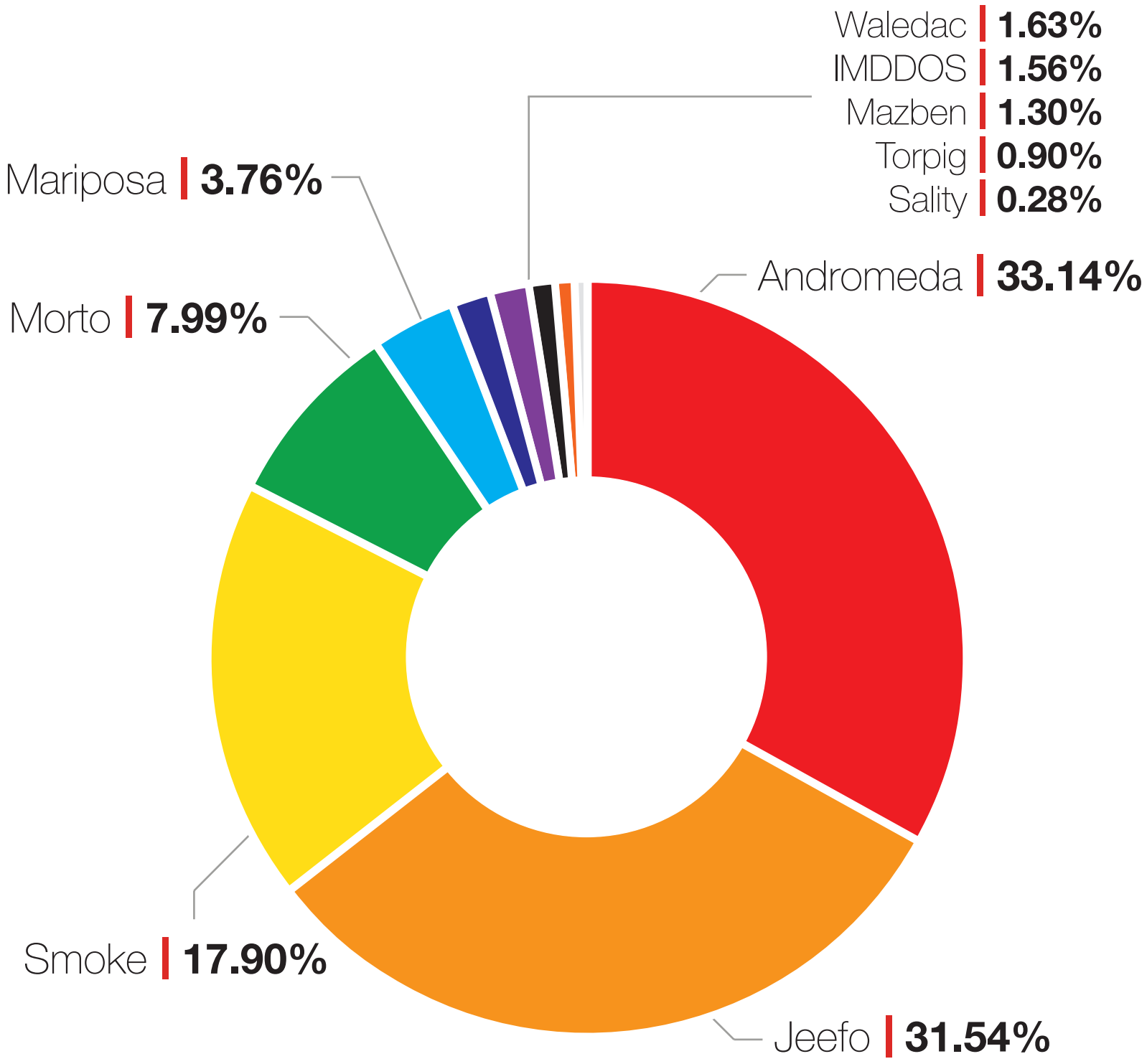
Earlier in 2013, we reported on the ZeroAccess botnet and how its controllers were **systematically adding about 100,000 new infections weekly** - leading us to believe that the person or persons behind it were not only paying a substantial amount of money weekly to generate new affiliate infections, but that they were able to make a significant amount of money doing so.[13] Like other cybercriminals, ZeroAccess's owners have taken pages from the playbooks of legitimate businesses and made successful attempts to diversify their income generation: we saw 32 and 64 bit versions of ZeroAccess being used to commit click fraud[14], search engine poisoning and to mine Bitcoin. With the dramatic rise in Bitcoin value over 2013, it's likely that the owners of ZeroAccess have profited substantially on the backs of their victims.

But that wasn't the end of the ZeroAccess story: we saw two separate attempts to take the botnet down. In July, Symantec attempted to kill the botnet, with limited success[15]. ZeroAccess's owners responded in turn with new versions of the bot and a massive spike in fresh infections. Late last year Microsoft and the European Cybercrime Centre launched an assault on the botnet[16], directed at the command and control infrastructure of the botnet. ZeroAccess's controllers were quick to respond with an update to counter the takedown, but Microsoft stuck back with a counterpunch of their own. Soon after, the criminals behind the botnet sent another update to their bots with the message WHITE FLAG, which seems to have been a message to surrender and cease the botnet's click fraud operations.[17]

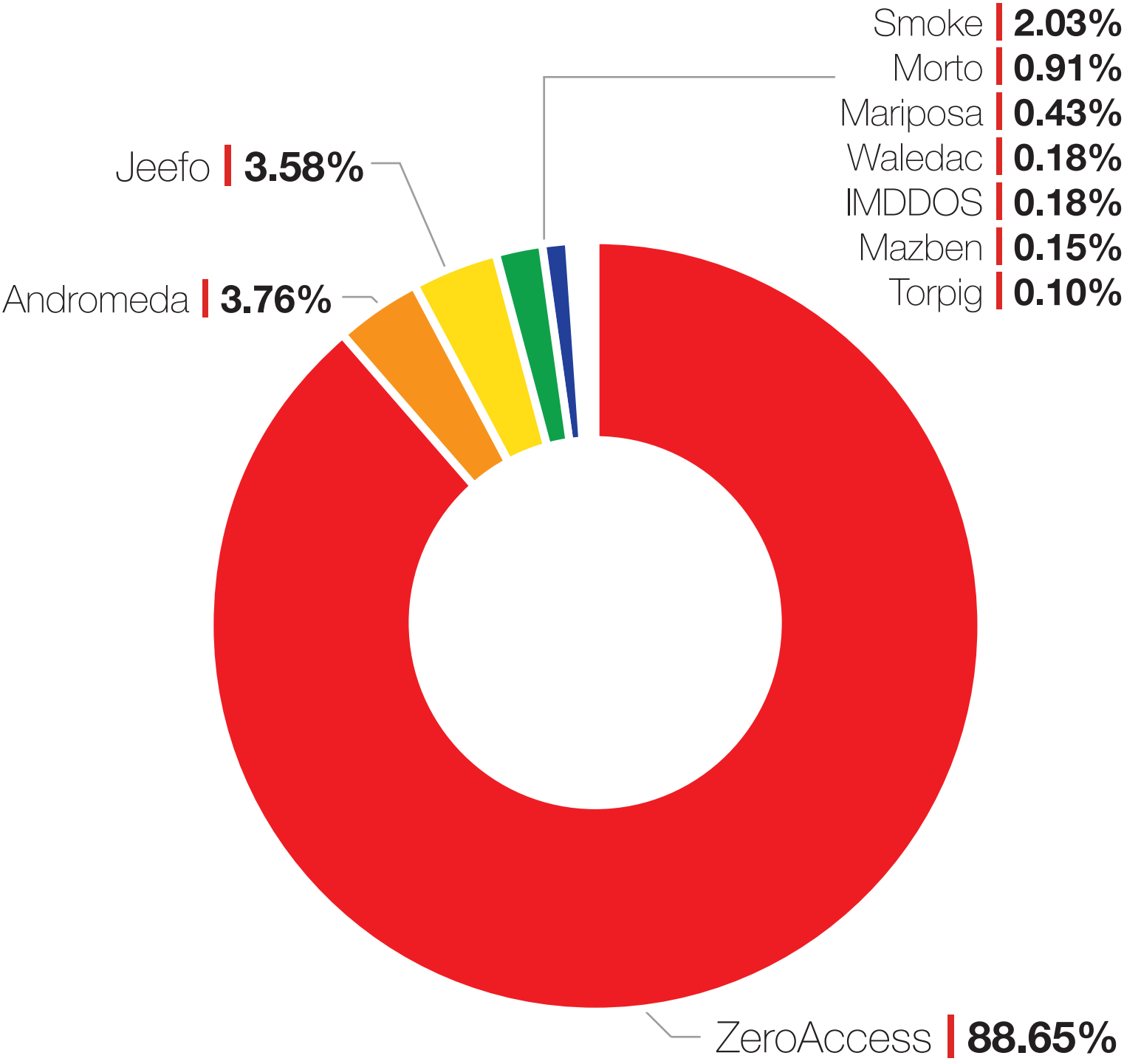
Since the takedown, our monitoring of the botnet has shown no new updates of the botnet, although a significant number of bots are still online and active, although that number is decreasing. Is ZeroAccess down for the count? Perhaps. But as we saw last year with other botnets thought to be long since dormant, there is little effort required to bring the beast back to life. With millions of dollars being made by ZeroAccess's owners, we suspect we haven't seen the last of ZeroAccess and its kind.


Botnet Incidents Recorded (excluding ZeroAccess)
Number of Alerts, Monthly, Millions
200
125
50
Jan
Feb
Mar
Apr
May
Jun
Jul
Aug
Sept
Oct
Nov
Dec

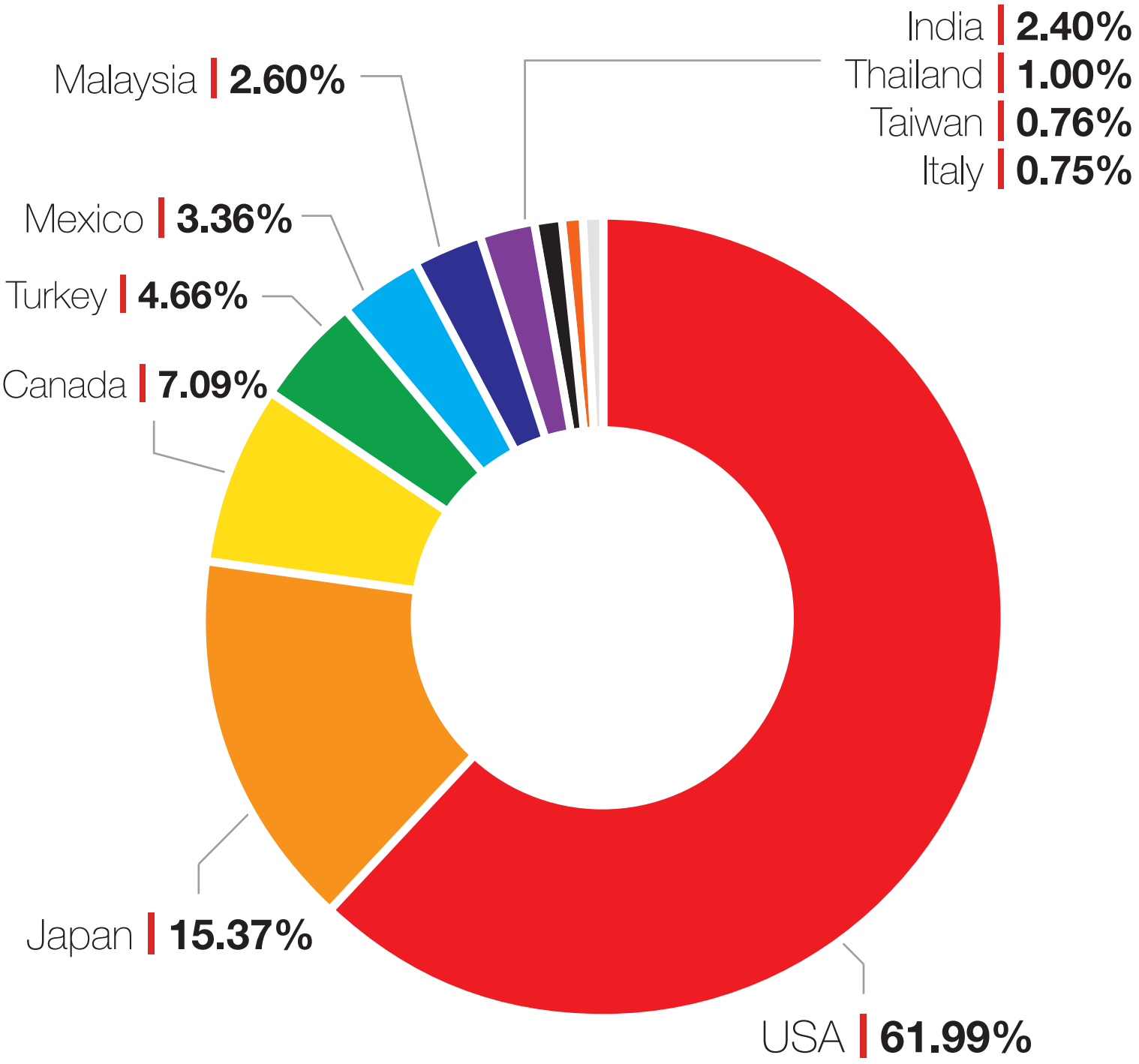

ZeroAccess Botnet Incidents Recorded
Number of Alerts, Monthly, Millions
3000
1750
500
Jan
Feb
Mar
Apr
May
Jun
Jul
Aug
Sept
Oct
Nov
Dec



Botnet Prevalence (excluding ZeroAccess), 2013



Botnet Prevalence including ZeroAccess, 2013

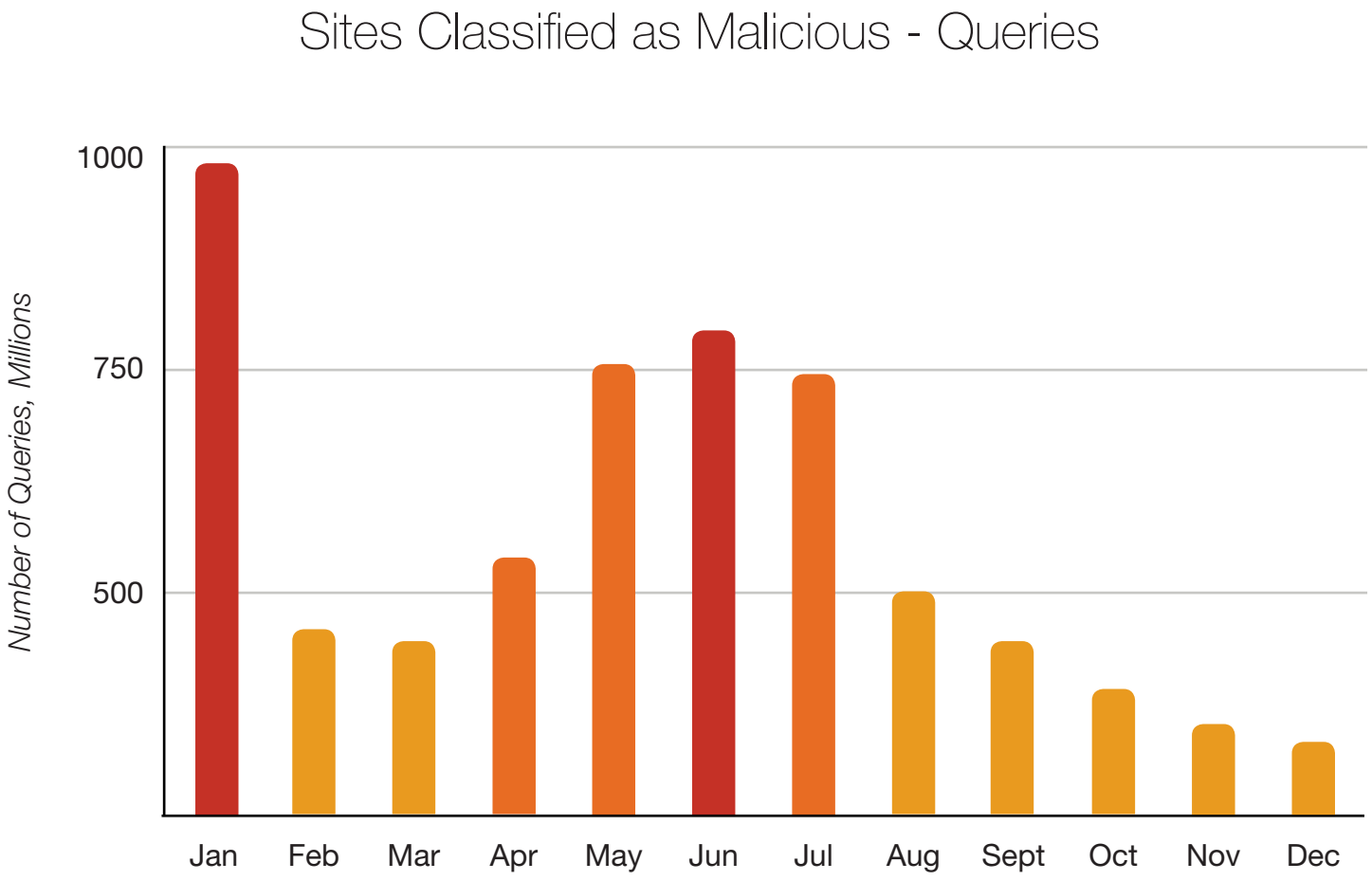


Top 10 Geographical Distribution, Botnet Incidents, 2013

Web:

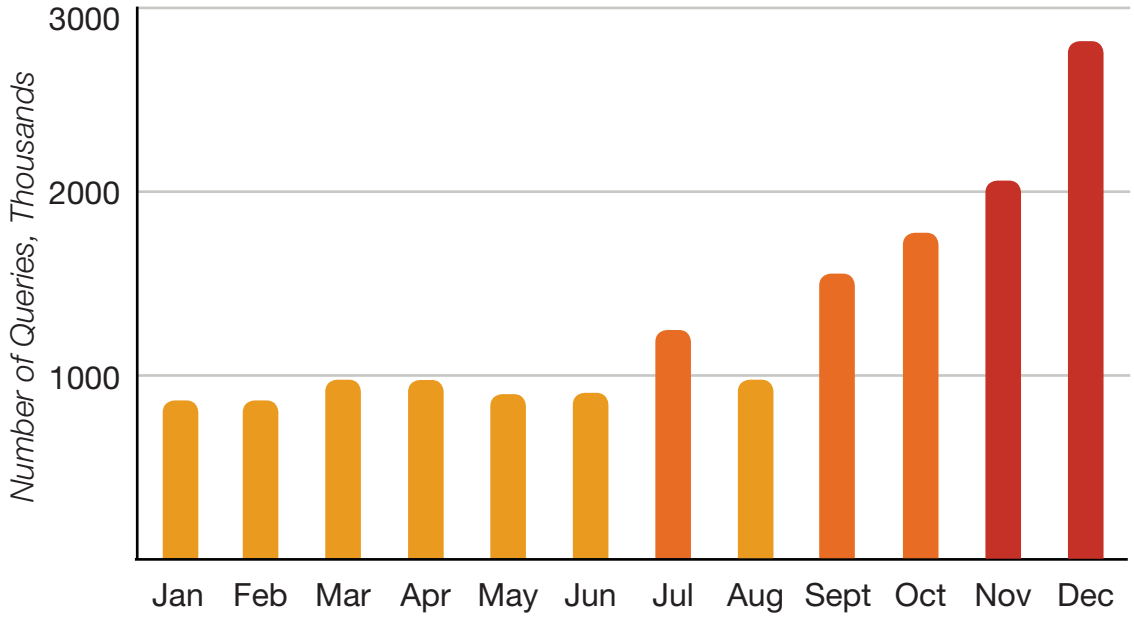
Billions (attempted to be) Served

In 2013, FortiGates around the world were kept very busy on the web filtering front. FortiGuard Labs added almost 20 million new sites and IP addresses to our classification lists, and updated over 64 million existing sites. As sites change, become subverted to deliver malware, clean themselves up after an attack or cease to exist, the FortiGuard team is quick to respond. It's easy to see that network administrators have no small task when it comes to ensuring their users steer clear of potentially malicious or legally questionable Internet properties. Every time a computer user attempts to access a site protected by a FortiGate, a query is sent to FortiGuard to determine what type of site it is and then if it is safe (or allowed) to visit.



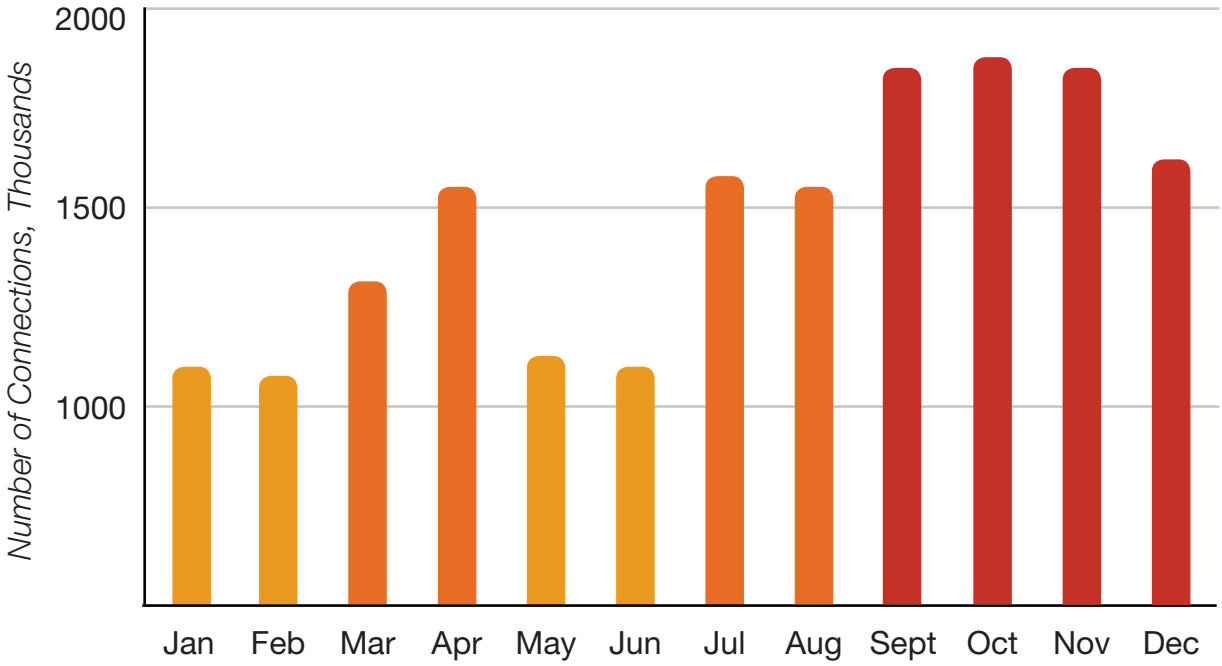
Websites that host software that is covertly or silently downloaded to a user's machine to collect information, monitor user activity, or hold data for ransom are classified as malicious. Sites that have been taken over or designed to infect targets with destructive or malicious software, that is specifically designed to damage, disrupt, attack or manipulate computer systems without the user's consent are such as a virus or trojan horse.

Sites Classified as Phishing - Queries



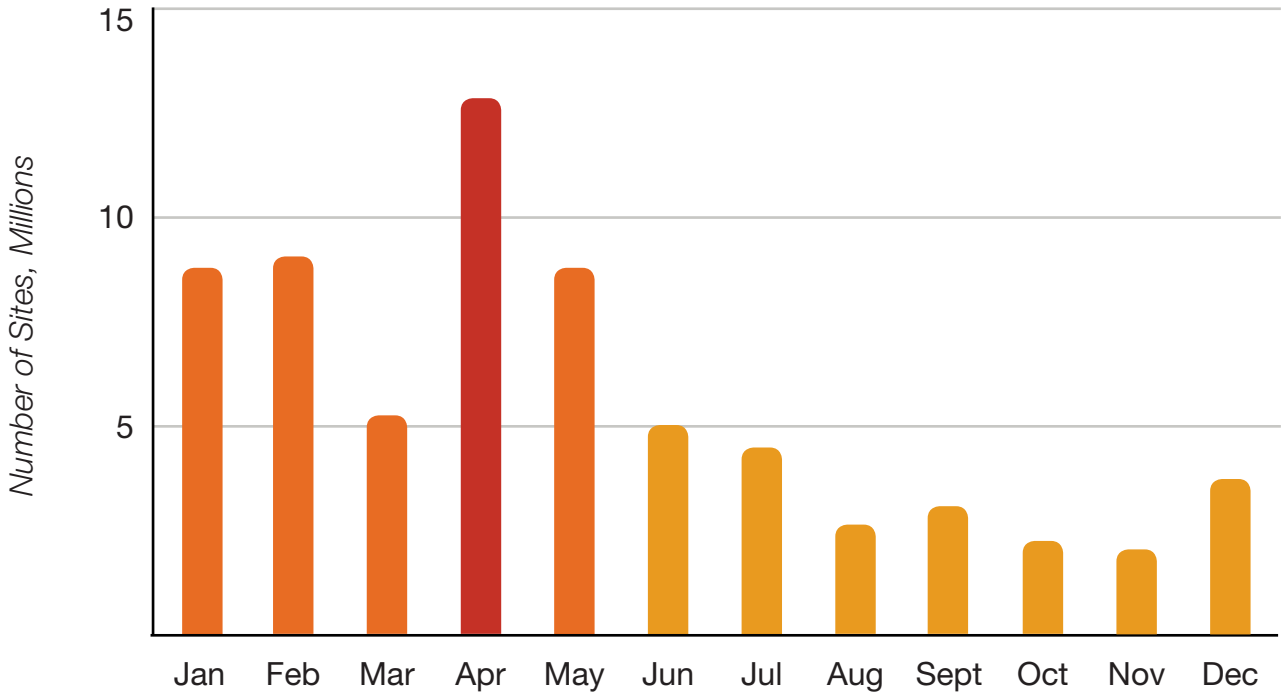
Phishing sites are counterfeit or other deceptive web pages that duplicate legitimate web pages for the purpose of stealing financial, personal or other private information from the users.

Sites Classified as Known Spam URLs - Queries

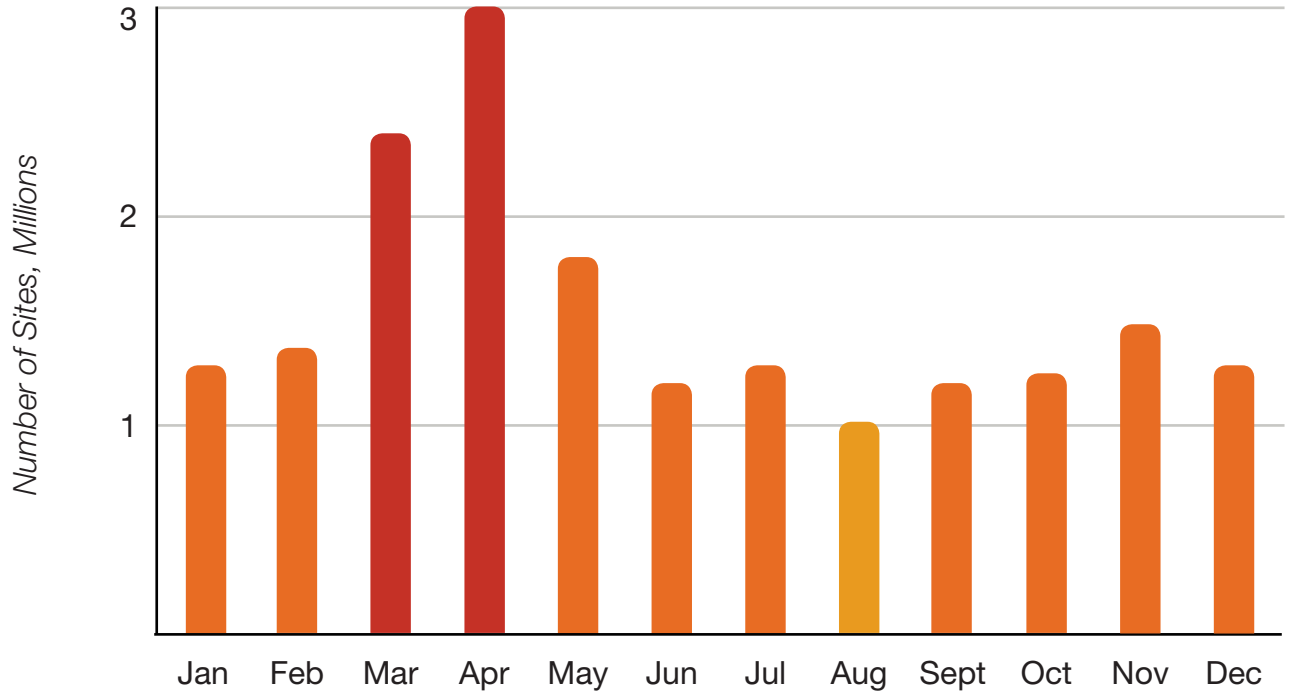


Spam sites are sites or pages whose URLs are found in spam emails. These webpages often advertise sex sites, fraudulent wares, and other potentially offensive materials.

Web Sites Updated, 2013



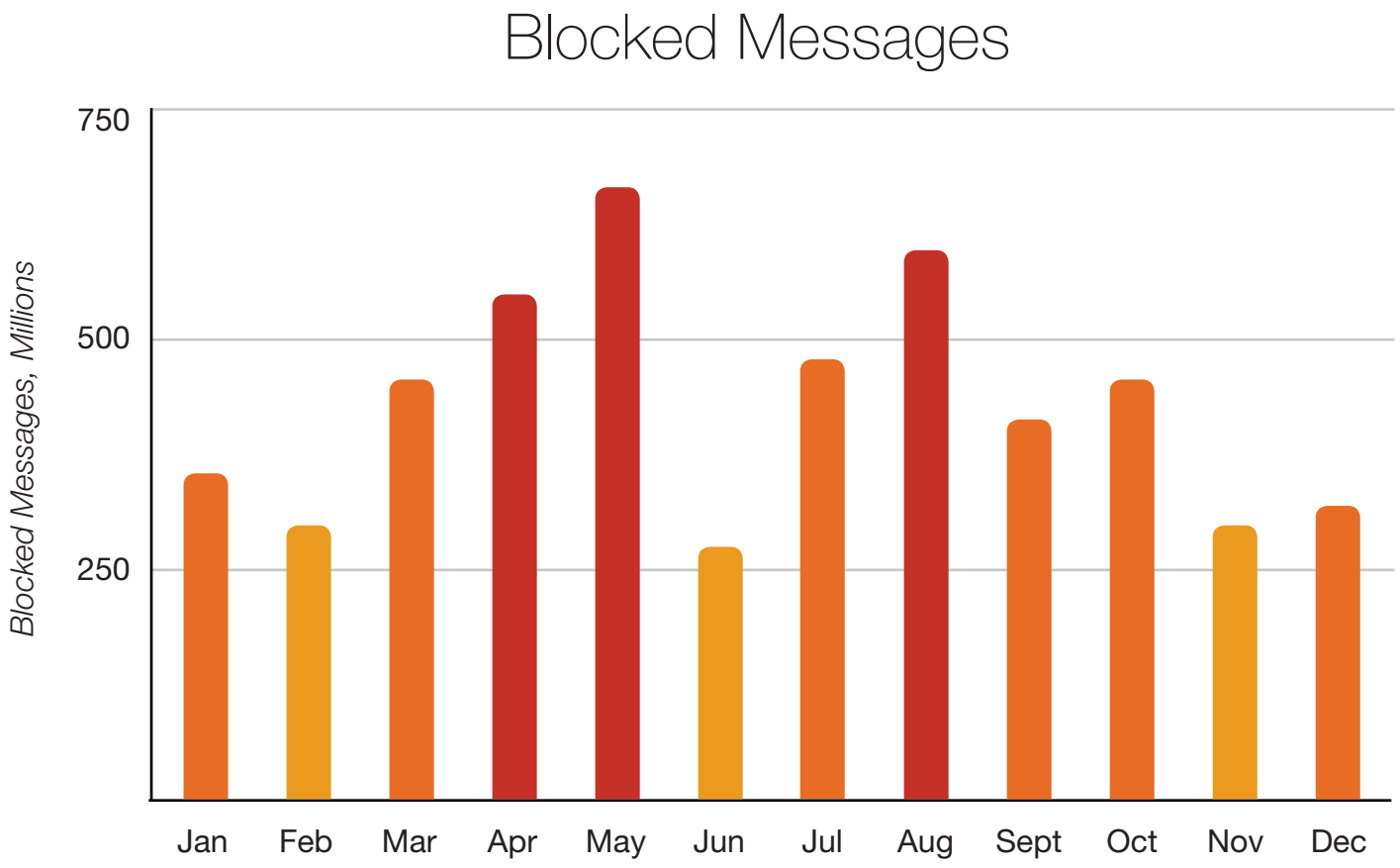
Web Sites Added, 2013



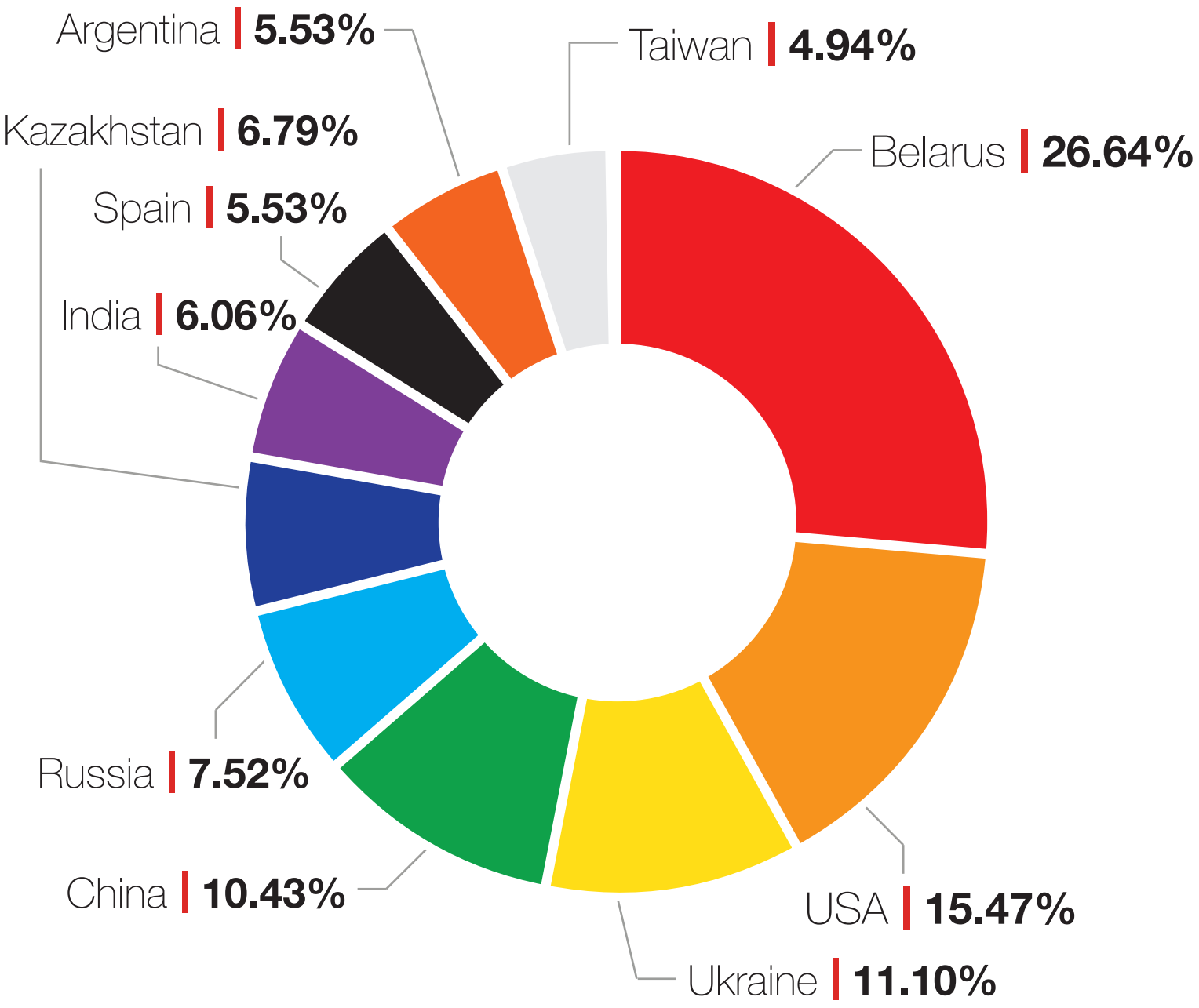
Spam:

Global Audience, Global Delivery

Spam: it's something we are all familiar with. We see it in our spam folders and occasionaly in our inboxes daily. Literally billions of messages are sent daily in the hopes that the message will make it through the automated systems designed to block them. Spammers will try multiple methods to foil scanners and to entice you to click on the links inside their messages: fake fax messages, pharmaceutical ads, e-cards and malicious attachments or links designed to deliver malware are all in the modern day spammer's toolkit. Perhaps what is most interesting is how diversified spammers are globally when it comes to sending their messages: our statistics shows that while about half of all messages we saw in 2013 came from Eastern Europe and Russia, the remaining countries in our top 10 are located all over the globe.

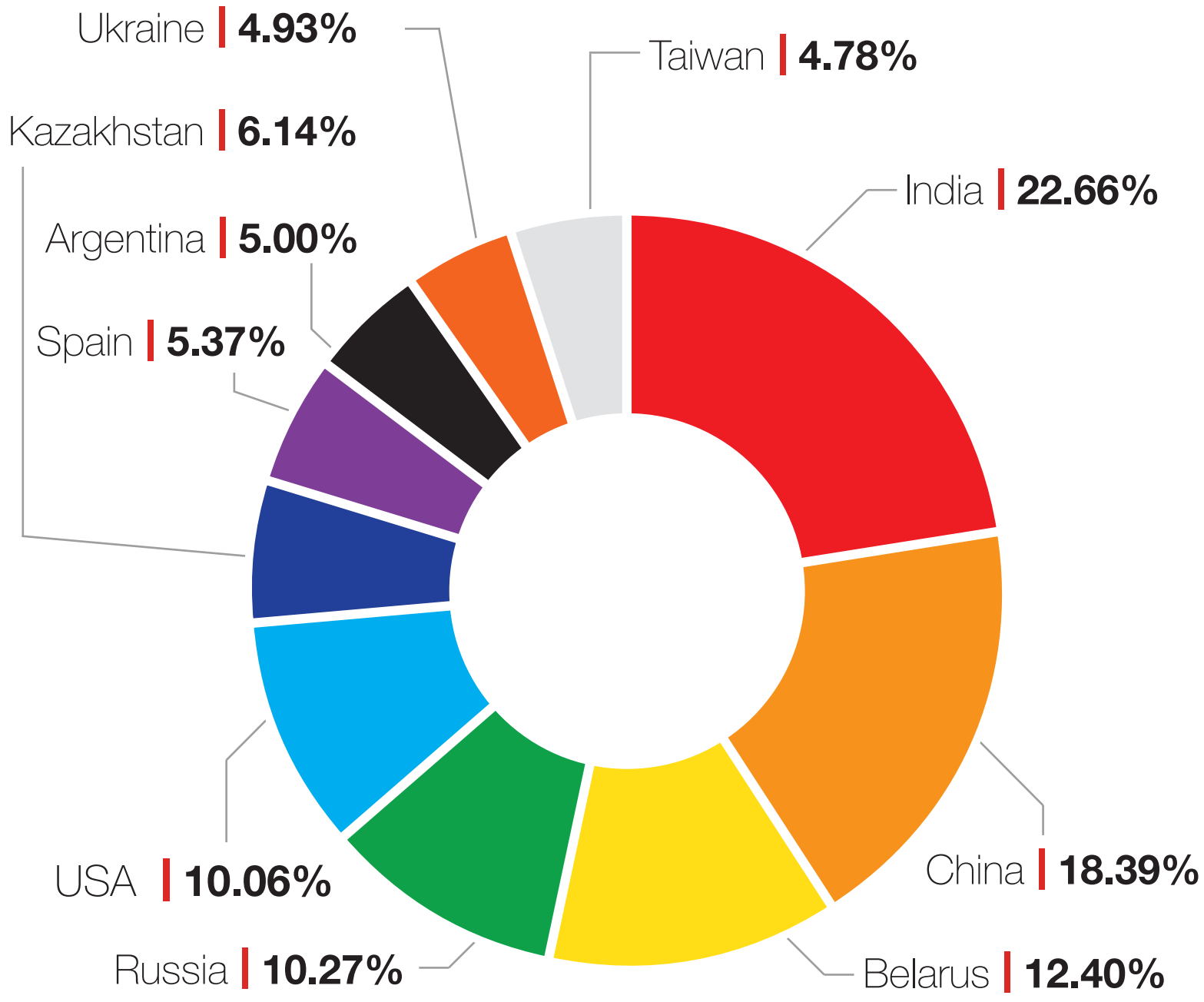


FortiGate and FortiMail devices around the world are designed to detect and prevent spam emails from appearing in inboxes of users. In 2013 Fortinet devices blocked billions of messages.



Total Number of Spam Messages by Country, Top 10, 2013

Senders of spam will attempt to send spam from anywhere they can, anywhere on the planet, using anything from an infected desktop being used as a relay to underground servers. Of the top 10 sources of spam recorded in 2013, over half originated from Eastern Europe and Russia.



Average Monthly Total of IPs Sending Spam, Top 10, 2013

When we look at the number of unique IP addresses being used to send spam per month, the picture is slightly different, but equally globally diversified - spammers build massive networks in the hopes of defeating antispam measures.

FortiGuard Labs:

Threat Research and Response

What Is FortiGuard Labs?

Fortinet is the only network security vendor to have its own global threat research & response team continuously monitoring the threat landscape and providing customers with real-time protection against the latest Internet threats. FortiGuard Labs' expert team of threat researchers is located around the world to deliver security updates 24/7, with industry leading response times to new and emerging threats targeting your network, content and mobile devices.

In a typical week, FortiGuard Labs creates or updates:

- 235,000 antivirus definitions
- 70 IPS signatures
- 725,000 URL ratings covering 69 languages
- 66 million new and updated antispam signatures.

Fortinet has more than 200 dedicated research analysts, engineers, and forensic specialists. Operating in security labs around the globe, the FortiGuard Labs provide 'follow-the-sun' worldwide coverage to assure industry-leading response times to new viruses, vulnerabilities, attacks, and malicious threats.

Fortinet's FortiGuard Labs constantly analyze the threat landscape and delivers original research - including discovery and responsible disclosure of zero-day vulnerabilities – as well as rapid signature updates to provide practically instant protection from new and emerging threats.

The team collects data from the FortiGate network security appliances and intelligence systems in production worldwide to identify threats. They are able to rapidly respond to discovered threats by pushing out signature updates to every Fortinet customer in the world within minutes. This is a unique Fortinet advantage since competing security companies do not have in-house security analysts and rely on third-party security companies to provide them with the latest malware signatures. In parallel, FortiGuard Labs constantly update its subscription services to proactively protect Fortinet's customers from network activities that may lead to vulnerabilities for their data and business assets.

On the research side, FortiGuard Labs has individuals dedicated to proactively researching the latest rootkits, botnets, packers and malware for both computers and mobile devices, enabling synergistic security intelligence and true zero-day protection from new and emerging threats. Here, the team also collaborates with the world's leading threat monitoring organizations (such as FIRST, KISA, Spamhaus, SRI, and Exodus Intelligence) and contributes to the overall security industry by identifying and responsibly reporting vulnerabilities directly to vendors of hardware, operating systems, and applications.

FortiGuard Labs - 2013 Year in Review

Zero-Day Research

FortiGuard protects against zero-day threats and APTs by providing proactive IPS detection well in advance of patches or updates provided by the affected vendor. FortiGuard Labs actively research and discover zero-day vulnerabilities in products which are likely candidates that a hacker would also uncover. Once the flaw is discovered, it is confidentially disclosed to the affected vendor under our Responsible Disclosure protocols. Our team proactively discovers these with the following goals:

1. Protect our customers via zero-day IPS for the zero-day flaws that we exclusively uncover. Since FortiGuard Labs discovers the actual Proof of Concept (POC), we can create protection well in advance of a vendor patch or update. It's an effective and important component of Advanced Persistent Threat protection.
2. We notify the vendor immediately via their PSIRT (or other means if PSIRT is unavailable)so that they may plan to patch the hole and protect their clients.
3. Reduce the number of holes that malicious attackers may find, adding resistance to their efforts.

Since research began in 2006, FortiGuard Labs has discovered 142 zero-day vulnerabilities, of which as of this writing 14 remain unpatched.

In 2013, we discovered and responsibly disclosed 18 new zero-day discoveries, of which 12 remain unpatched. The majority of these vulnerabilities were classified as Important or Critical.[18]

Effected Vendor	Risk	Reported	Vendor Patch Available	Effected Vendor	Risk	Reported	Vendor Patch Available
Apple	4	01/18/13	Yes - 09/23/13	Apple	4	06/06/13	No
Apple	4	01/22/13	Yes - 09/23/13	Cisco	4	07/29/13	No
Apple	3	01/29/13	No	Adobe	5	01/29/13	Yes - 09/11/13
Adobe	5	03/05/13	Yes - 04/10/13	Cisco	3	09/16/13	No
Microsoft	5	03/26/13	No	Cisco	3	11/08/13	No
Adobe	5	05/06/13	Yes - 07/15/13	Adobe	5	11/19/13	No
Apple	5	05/21/13	Yes - 09/23/13	Adobe	5	11/19/13	No
Apple	4	06/06/13	No	Adobe	4	12/12/13	No
Apple	4	06/06/13	No	Adobe	3	12/12/13	No

Industry Leading Malware Analysis

FortiGuard Labs also maintains a large, dedicated team of antivirus and malware researchers and analysts whose chief role is to obtain, review, analyze and reverse engineer malware in order to stay abreast of new developments in malware development.

As part of that role, our analysts are proud to share these findings to the antimalware community at large through the industry trade publication, *Virus Bulletin*. Virus Bulletin, first published in 1989, is a publication devoted to information on the prevention, detection and removal of malware.

In 2013, FortiGuard Labs were proud to have 19 features in issues of Virus Bulletin.[19]

FortiGuard Labs Published Papers - 2013 Issues of Virus Bulletin

January:
Talk to You Later, Raul Alvarez

February:
Please Help!, Raul Alvarez

March:
The Evolution of Zortob, Dong Xie

April:
Pushdo's New Second Generation, Neo Tan, He Xu & Kyle Yang

May:
A Good Look at the Andromeda Botnet, He Xu

Persistency in the Wild, Raul Alvarez

Cat-and-Mouse Game in CVE-2012-0158, Ruhai Zhang

June:
Chat-and-Paste, Raul Alvarez

Bitcoin Mining: Investing in the Future of the Underground Market, Micky Pun

July:
Who's Bad? Skybot or Ngrbot, Neo Tan, Christy Chung & Kyle Yang

Unlocking Lockscreen, Walter (Tiezhu) Kong & Kyle Yang

August:
Andromeda 2.7 Features, Suweera DeSouza & Neo Tan

The ZeroAccess Money-Generating Campaign, Chao Chen & Kyle Yang

September:
Nedsym Spamming, He Xu

October:
Same Zeus, Different Features, Raul Alvarez

November:
Neurevt Bot Analysis, Zhongchun Huo

When ZAccess Becomes a Debugger, He Xu

December:
Onkod: A Downloader and its 'Downloadee', Raul Alvarez

Fake KakaoTalk Security Plug-in, Zhe Li & Dong Xie

Fortinet (NASDAQ: **FTNT**) is a worldwide provider of network security appliances and a market leader in unified threat management (UTM). Our products and subscription services provide broad, integrated and high-performance protection against dynamic security threats while simplifying the IT security infrastructure. Our customers include enterprises, service providers and government entities worldwide, including the majority of the 2011 Fortune Global 100. Fortinet is headquartered in Sunnyvale, Calif., with offices around the world.

Founded in 2000 by Ken Xie, the visionary founder and former president and CEO of NetScreen, Fortinet is led by a strong and seasoned management team with deep experience in networking and security. Fortinet's market position has been validated by widespread recognition by industry analysts, business organizations, and media.

Fortinet's flagship FortiGate® security platforms offer a powerful blend of ASIC-accelerated performance, integrated multi-threat response, and constantly-updated, in-depth threat intelligence. Employing innovative technologies for networking, security and content analysis, Fortinet systems integrate the industry's broadest suite of security technologies, including firewall, VPN, antivirus, intrusion prevention (IPS), application control, Web filtering, antispam, wireless controller, and WAN acceleration, all of which can be deployed individually to complement legacy solutions or combined for a comprehensive threat management solution. The company complements these solutions with an array of management, analysis, e-mail, database and end-point security products.

A key differentiator, Fortinet's custom-built FortiASIC content and network processors enable FortiGate systems to detect and eliminate even complex, blended threats in real time without degrading network performance, while an extensive set of complementary management, analysis, database and endpoint protection solutions increases deployment flexibility, assists in compliance with industry and government regulations, and reduces the operational costs of security management.

To date, Fortinet has shipped more than 1,300,000 appliances to more than 170,000 customers worldwide, including:

- 61 of the Global 100
- 8 of the top 10 Fortune companies in Americas
- 9 of the top 10 Fortune companies in EMEA
- 9 of the top 10 Fortune companies in APAC
- 7 of the top 10 Fortune telecommunications companies
- 9 of the top 10 Fortune banking companies
- 9 of the top 10 Fortune defense/ aerospace companies

Fortinet is headquartered in Sunnyvale, California, with customer support, development and sales facilities throughout the world. Fortinet sells its system and subscription service products through a network of channel partners worldwide.

References

1. 2013 Fortinet Cybercrime Report
http://www.fortinet.com/resource_center/whitepapers/cybercrime_report_on_botnets_network_security_strategies.html

2. Disk encrypting Cryptolocker malware demands $300 to decrypt your files
http://www.geek.com/apps/disk-encryptiing-cryptolocker-malware-demands-300-to-decrypt-your-files-1570402/

3. Blackhole malware kingpin 'Paunch' arrested in Russia
http://rt.com/news/blackhole-paunch-arrest-russia-946/

4. Police Arrest Alleged ZeuS Botmaster "bx1"
http://krebsonsecurity.com/2013/01/police-arrest-alleged-zeus-botmaster-bx1/

5. Suspected hackers behind Carberp botnet, Eurograbber arrested
http://www.zdnet.com/suspected-hackers-behind-carberp-botnet-eurograbber-arrested-7000013580/

6. Carberp Source Code Leak Likely to Spawn Malware Variants, Innovation
http://www.darkreading.com/endpoint/carberp-source-code-leak-likely-to-spawn/240157400

7. Exclusive: Ongoing malware attack targeting Apache hijacks 20,000 sites
http://arstechnica.com/security/2013/04/exclusive-ongoing-malware-attack-targeting-apache-hijacks-20000-sites/

8. Grappling with the ZeroAccess Botnet
http://www.symantec.com/connect/blogs/grappling-zeroaccess-botnet

9. Zeus Source Code Leaked
http://threatpost.com/zeus-source-code-leaked-051011

10. CryptoLocker's crimewave: A trail of millions in laundered Bitcoin
http://www.zdnet.com/cryptolockers-crimewave-a-trail-of-millions-in-laundered-bitcoin-7000024579/

11. A Day in the Life of a Mobile Ransomware
http://blog.fortinet.com/Ransomware/

12. Virut and Waledac Botnets Spamming from Shared Machines
http://threatpost.com/virut-and-waledac-botnets-spamming-shared-machines-011513/

13. FortiGuard Midyear Threat Report
http://www.fortinet.com/resource_center/whitepapers/quarterly-threat-landscape-report-q213.html

14. New ZeuS Banking Trojan Targets 64-Bit Systems, Leverages Tor
http://www.darkreading.com/attacks-breaches/new-zeus-banking-trojan-targets-64-bit-s/240164713

15. 'Quarter' of TWO-MILLION-strong zombie PC army lured to their deaths
http://www.theregister.co.uk/Print/2013/10/01/zeroaccess_botnet_sunk_sorta/

16. Microsoft, the FBI, Europol and industry partners disrupt the notorious ZeroAccess botnet
http://www.microsoft.com/en-us/news/press/2013/dec13/12-05zeroaccessbotnetpr.aspx

17. ZeroAccess Crew Throws Up 'White Flag' After Botnet Takedown
http://www.eweek.com/security/zeroaccess-crew-throws-up-white-flag-after-botnet-takedown.html

18. FortiGuard Center - Threat Research & Response
http://www.fortiguard.com/static/intrusionprevention.html

19. Virus Bulletin Magazine - Archive
https://www.virusbtn.com/virusbulletin/archive/index

GLOBAL HEADQUARTERS
Fortinet Inc.
1090 Kifer Road
Sunnyvale, CA 94086
United States
Tel: +1.408.235.7700
Fax: +1.408.235.7737
www.fortinet.com/sales

EMEA SALES OFFICE
120 rue Albert Caquot
06560, Sophia Antipolis,
France
Tel: +33.4.8987.0510
Fax: +33.4.8987.0501

APAC SALES OFFICE
300 Beach Road 20-01
The Concourse
Singapore 199555
Tel: +65.6513.3730
Fax: +65.6223.6784

LATIN AMERICA SALES OFFICE
Prol. Paseo de la Reforma 115 Int. 702
Col. Lomas de Santa Fe,
C.P. 01219
Del. Alvaro Obregón
México D.F.
Tel: 011-52-(55) 5524-8480

Copyright© 2014 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, and FortiGuard®, are registered trademarks of Fortinet, Inc., and other Fortinet names herein may also be trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance metrics contained herein were attained in internal lab tests under ideal conditions, and performance may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's General Counsel, with a purchaser that expressly warrants that the identified product will perform according to the performance metrics herein. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. Fortinet disclaims in full any guarantees. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.